

EXHIBIT 7

[Table of Contents](#)

As filed with the Securities and Exchange Commission on August 6, 2021

Registration No. 333-256129

**UNITED STATES
SECURITIES AND EXCHANGE COMMISSION**
Washington, D.C. 20549

**AMENDMENT NO. 3
TO
FORM S-4
REGISTRATION STATEMENT
UNDER
THE SECURITIES ACT OF 1933**

LGL SYSTEMS ACQUISITION CORP.

(Exact name of Registrant as specified in its charter)

Delaware
(State or other jurisdiction of
incorporation or organization)

7372
(Primary standard industrial
classification code number)

83-459946
(I.R.S. Employer
Identification Number)

165 W. Liberty Street, Suite 220
Reno, NV 89501

Telephone: (705) 393-9113

(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

Robert V. "Rob" LaPenta Jr.
Co-Chief Executive Officer and Chief Financial Officer
LGL Systems Acquisition Corp.
165 W. Liberty Street, Suite 220
Reno, NV 89501
Telephone: (705) 393-9113

(Name, address, including zip code, and telephone number, including area code, of agent for service)

With copies to:

Michael L. Zuppone
Luke P. Iovine, III
Keith D. Pisani
Paul Hastings LLP
200 Park Avenue
New York, NY 10166
(212) 318-6000

Brian F. Leaf
Garth A. Osterman
Cooley LLP
One Freedom Square
Reston Town Center
11951 Freedom Drive
Reston, VA 20190
(703) 456-8000

Approximate date of commencement of proposed sale of the securities to the public: As soon as practicable after this Registration Statement becomes effective and all other conditions to the transactions contemplated by the Agreement and Plan of Reorganization and Merger described in the included proxy statement/prospectus have been satisfied or waived.

If the securities being registered on this form are to be offered in connection with the formation of a holding company and there is compliance with General Instruction G, check the following box: ☐

If this form is filed to register additional securities for an offering pursuant to Rule 462(b) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this form is a post-effective amendment filed pursuant to Rule 462(d) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☐
Non-accelerated filer ☒

Accelerated filer ☐
Smaller reporting company ☒
Emerging growth company ☒

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 7(a)(2)(B) of the Securities Act. ☐

If applicable, place an X in the box to designate the appropriate rule provision relied upon in conducting this transaction:

Exchange Act Rule 13e-4(i) (Cross-Border Issuer Tender Offer) ☐

Exchange Act Rule 14d-1(d) (Cross-Border Third-Party Tender Offer) ☐

The registrant hereby amends this registration statement on such date or dates as may be necessary to delay its effective date until the registrant shall file a further amendment which specifically states that this registration statement shall thereafter become effective in accordance with Section 8(a) of the Securities Act of 1933, as amended, or until the registration statement shall become effective on such date as the Securities and Exchange Commission, acting pursuant to said Section 8(a), may determine.

[Table of Contents](#)

IF YOU RETURN YOUR PROXY CARD WITHOUT AN INDICATION OF HOW YOU WISH TO VOTE, YOUR SHARES WILL BE VOTED IN FAVOR OF EACH OF THE PROPOSALS.

ALL LGL PUBLIC STOCKHOLDERS HAVE THE RIGHT TO HAVE THEIR SHARES REDEEMED FOR CASH IN CONNECTION WITH THE PROPOSED BUSINESS COMBINATION. PUBLIC STOCKHOLDERS ARE NOT REQUIRED TO AFFIRMATIVELY VOTE FOR OR AGAINST THE BUSINESS COMBINATION PROPOSAL OR BE HOLDERS OF RECORD ON THE RECORD DATE IN ORDER TO HAVE THEIR SHARES REDEEMED FOR CASH. THIS MEANS THAT ANY PUBLIC STOCKHOLDER HOLDING SHARES OF LGL COMMON STOCK MAY EXERCISE REDEMPTION RIGHTS REGARDLESS OF WHETHER THEY ARE EVEN ENTITLED TO VOTE ON THE BUSINESS COMBINATION PROPOSAL.

TO EXERCISE REDEMPTION RIGHTS, HOLDERS MUST TENDER THEIR STOCK TO CONTINENTAL STOCK TRANSFER & TRUST COMPANY, LGL'S TRANSFER AGENT, NO LATER THAN TWO BUSINESS DAYS PRIOR TO THE SPECIAL MEETING. YOU MAY TENDER YOUR STOCK EITHER BY DELIVERING YOUR STOCK CERTIFICATE TO THE TRANSFER AGENT OR BY DELIVERING YOUR SHARES ELECTRONICALLY USING THE DEPOSITORY TRUST COMPANY'S DEPOSIT WITHDRAWAL AT CUSTODIAN SYSTEM. IF THE BUSINESS COMBINATION IS NOT COMPLETED, THEN THESE SHARES WILL NOT BE REDEEMED FOR CASH. IF YOU HOLD THE SHARES IN "STREET NAME," YOU WILL NEED TO INSTRUCT THE ACCOUNT EXECUTIVE AT YOUR BANK OR BROKER TO WITHDRAW THE SHARES FROM YOUR ACCOUNT IN ORDER TO EXERCISE YOUR REDEMPTION RIGHTS. SEE THE SECTION ENTITLED "*SPECIAL MEETING OF LGL STOCKHOLDERS—REDEMPTION RIGHTS*" FOR MORE SPECIFIC INSTRUCTIONS.

[Table of Contents](#)

The information in this proxy statement/prospectus is not complete and may be changed. We may not issue these securities until the registration statement filed with the Securities and Exchange Commission is effective. This proxy statement/prospectus is not an offer to sell these securities, and it is not soliciting an offer to buy these securities in any jurisdiction where the offer or sale is not permitted.

SUBJECT TO COMPLETION, DATED AUGUST 6, 2021

PROXY STATEMENT FOR SPECIAL MEETING OF LGL SYSTEMS ACQUISITION CORP.

PROSPECTUS FOR UP TO 86,340,000 SHARES OF COMMON STOCK

The board of directors of each of LGL Systems Acquisition Corp., a Delaware corporation (“LGL”), and IronNet Cybersecurity, Inc., a Delaware corporation (“IronNet”), has unanimously approved the Agreement and Plan of Reorganization and Merger, dated as of March 15, 2021, as amended by Amendment No. 1 to Agreement and Plan of Reorganization and Merger dated as of August 6, 2021 (as may from time to time be further amended, restated, supplemented or otherwise modified, the “*Merger Agreement*”), by and among LGL, LGL Systems Merger Sub Inc., a Delaware corporation and wholly owned subsidiary of LGL (“*Merger Sub*”), and IronNet, pursuant to which Merger Sub will merge with and into IronNet, with IronNet surviving as a wholly owned subsidiary of LGL (the “*Business Combination*”, and the post-Business Combination entity being referred to as “LGL” or the “*Combined Company*”). Upon the closing of the Business Combination, LGL intends to change its name from “LGL Systems Acquisition Corp.” to “IronNet, Inc.”

Pursuant to the Merger Agreement, (i) each outstanding share of IronNet common stock and IronNet preferred stock (with each share of IronNet preferred stock being treated as if it were converted into ten (10) shares of IronNet common stock on the effective date of the Business Combination) will be converted into the right to receive (a) a number of shares of LGL common stock equal to the exchange ratio, the numerator of which is \$863,400,000 divided by \$10.00, and the denominator of which is equal to the number of shares of IronNet common stock on a fully-diluted basis as of immediately prior to the effective time of the Business Combination, including shares of IronNet common stock issuable upon conversion/exercise of outstanding IronNet options, IronNet warrants, IronNet restricted stock units and IronNet restricted stock awards (in each case, whether or not vested) and (b) a cash amount payable in respect of fractional shares of LGL common stock that would otherwise be issued in connection with the foregoing conversion, if applicable, and (ii) each IronNet option, IronNet restricted stock unit, IronNet restricted stock award or IronNet warrant that is outstanding immediately prior to the closing of the transactions (and by its terms will not terminate upon the closing of the transactions) will remain outstanding and thereafter (x) in the case of options, represent the right to purchase a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such option multiplied by the same exchange ratio used for IronNet common stock (rounded down to the nearest whole share) at an exercise price per share equal to the current exercise price per share for such option divided by such exchange ratio (rounded up to the nearest whole cent), (y) in the case of warrants, represent the right to purchase a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such warrant multiplied by such exchange ratio, multiplied by ten (10) at an exercise price equal to the current exercise price per share (rounded up to the nearest whole cent) for such warrant divided by such exchange ratio, divided by ten (10) (rounded down to the nearest whole share), and (z) in the case of stock units and restricted stock awards, represent a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such stock unit or restricted stock award multiplied by such exchange ratio (rounded down to the nearest whole share). In addition, IronNet stockholders and eligible holders of options, warrants, restricted stock unit awards and restricted stock awards (as applicable, only to the extent time vested as of the closing of the Business Combination) may also receive as additional merger consideration a pro rata portion of 1,078,125 additional shares of LGL common stock if the volume weighted average share price for LGL’s common stock equals or exceeds \$13.00 for ten (10) consecutive days during the two year period following the closing of the Business Combination (the “*Earnout Shares*”).

If calculated based on the capitalization of IronNet as of July 31, 2021, the exchange ratio is approximately 0.8128 of a share of LGL common stock per fully-diluted share of IronNet common stock.

Proposals to approve and adopt the Merger Agreement and the other matters discussed in this proxy statement/prospectus will be presented for approval by LGL stockholders at the special meeting of stockholders of LGL scheduled to be held on August 26, 2021, in virtual format and approval by IronNet stockholders via written consent.

On March 15, 2021, LGL executed subscription agreements with certain investors for the sale of an aggregate of 12,500,000 shares of LGL common stock in a private placement transaction at a purchase price of \$10.00 per share for aggregate gross cash proceeds of \$125 million. The closing of the sale of these shares will occur concurrently with the consummation of the Business Combination. Of the amounts subscribed for in the private placement, the Sponsor has agreed to purchase 566,000 shares of Class A common stock for \$5,660,000.

LGL’s Class A common stock, redeemable warrants exercisable for shares of Class A common stock at an exercise price of \$11.50 per share, and units (each consisting of one share of Class A common stock and one-half of one redeemable warrant), are currently listed on the New York Stock Exchange (the “NYSE”) under the symbols DFNS, DFNS.WS and DFNS.U, respectively. Upon the closing of the Business Combination, it is contemplated that LGL will have a single class of common stock. LGL intends to apply for listing on the NYSE, to be effective at the consummation of the Business Combination, of the common stock to be issued in connection with the Business Combination (including the common stock issued pursuant to the related private placement) together with the common stock previously issued in its initial public offering, the warrants issued in its initial public offering and simultaneous private placement, and the common stock underlying the warrants issued in its initial public offering and simultaneous private placement, under the proposed symbols IRNT, in the case of the common stock, and IRNT.WS, in the case of the warrants. LGL will not have units traded on the NYSE following consummation of the Business Combination. It is a condition of the consummation of the Business Combination that the LGL common stock is approved for listing on the NYSE (subject only to official notice of issuance thereof and public holder requirements), but there can be no assurance such listing condition will be met. If such listing condition is not met, the Business Combination will not be consummated unless the listing condition set forth in the Merger Agreement is waived by the parties to that agreement.

LGL is an “emerging growth company” as defined in the Jumpstart Our Business Startups Act of 2012, as amended (the “JOBS Act”), and has elected to comply with certain reduced public company reporting requirements.

This proxy statement/prospectus provides you with detailed information about the Business Combination and other matters to be considered at the special meeting of LGL stockholders and by IronNet stockholders. We encourage you to carefully read this entire document. **You should also carefully consider the risk factors described in the section entitled “Risk Factors” beginning on page 36. These securities have not been approved or disapproved by the Securities and Exchange Commission or any state securities commission nor has the Securities and Exchange Commission or any state securities commission passed upon the accuracy or adequacy of this proxy statement/prospectus. Any representation to the contrary is a criminal offense.**

This proxy statement/prospectus is dated August 6, 2021, and is first being mailed to LGL stockholders on or about such date.

[Table of Contents](#)

IMPORTANT NOTE ABOUT THIS PROXY STATEMENT/ PROSPECTUS

This document, which forms part of a registration statement on Form S-4 filed with the SEC by LGL (File No. 333-256129) (the “Registration Statement”), constitutes a prospectus of LGL under Section 5 of the Securities Act, with respect to the shares of LGL common stock to be issued if the Business Combination described herein is consummated. This document also constitutes a notice of meeting and a proxy statement/prospectus under Section 14(a) of the Exchange Act with respect to the special meeting of LGL stockholders at which LGL stockholders will be asked to consider and vote upon a proposal to approve the Business Combination by the approval and adoption of the Merger Agreement, among other matters.

You should rely only on the information contained in this proxy statement/prospectus in determining whether to vote in favor of the Business Combination and the other proposals. No one has been authorized to provide you with information that is different from that contained in this proxy statement/prospectus. This proxy statement/prospectus is dated August 6, 2021. You should not assume that the information contained in this proxy statement/prospectus is accurate as of any date other than that date. Neither the mailing of this proxy statement/prospectus to LGL stockholders or IronNet stockholders nor the issuance by LGL of common stock in connection with the Business Combination will create any implication to the contrary.

[Table of Contents](#)**FORWARD-LOOKING STATEMENTS**

LGL believes it is important to communicate its expectations to its stockholders. However, there may be events in the future that LGL is not able to predict accurately or over which it has no control. Certain statements in this proxy statement/prospectus may constitute “forward-looking statements” for purposes of the federal securities laws. LGL’s forward-looking statements include, but are not limited to, statements regarding LGL, LGL’s management team’s, IronNet’s and IronNet’s management team’s expectations, hopes, beliefs, intentions or strategies regarding the future. In addition, any statements that refer to projections, forecasts or other characterizations of future events or circumstances, including any underlying assumptions, are forward-looking statements. The words “anticipate,” “believe,” “continue,” “could,” “estimate,” “expect,” “intends,” “may,” “might,” “plan,” “possible,” “potential,” “predict,” “project,” “should,” “will,” “would” and similar expressions may identify forward-looking statements, but the absence of these words does not mean that a statement is not forward-looking. Forward-looking statements in this proxy statement/prospectus may include, for example, statements about:

- our ability to consummate the Business Combination;
- the anticipated timing of the Business Combination;
- the expected benefits of the Business Combination;
- the Combined Company’s financial and business performance following the Business Combination, including financial projections and business metrics;
- changes in the Combined Company’s strategy, future operations, financial position, estimated revenue and losses, projected costs, prospects and plans;
- the implementation, market acceptance and success of the Combined Company’s business model and growth strategy;
- IronNet’s expectations and forecasts with respect to the size and growth of the cybersecurity industry and IronNet’s products and services in particular;
- the ability of IronNet’s products and services to meet customers’ needs;
- IronNet’s ability to compete with others in the cybersecurity industry;
- IronNet’s ability to retain pricing power with its products;
- IronNet’s ability to grow its market share;
- the Combined Company’s ability to attract and retain qualified employees and management;
- the Combined Company’s ability to adapt to changes in consumer preferences, perception and spending habits and develop and expand its product offerings and gain market acceptance of its products, including in new geographies;
- the Combined Company’s ability to develop and maintain IronNet’s brand and reputation;
- developments and projections relating to IronNet’s competitors and industry;
- the impact of the COVID-19 pandemic on IronNet’s business and on the economy in general;
- IronNet’s expectations regarding its ability to obtain and maintain intellectual property protection and not infringe on the rights of others;
- expectations regarding the time during which the Combined Company will be an emerging growth company and a smaller reporting company under SEC rules;
- the Combined Company’s future capital requirements and sources and uses of cash;
- the Combined Company’s ability to obtain funding for its operations and future growth; and
- the Combined Company’s business, expansion plans and opportunities.

Table of Contents

These forward-looking statements are based on information available as of the date of this proxy statement/prospectus, and current expectations, forecasts and assumptions, and involve a number of judgments, risks and uncertainties. Accordingly, forward-looking statements should not be relied upon as representing our views as of any subsequent date, and we do not undertake any obligation to update forward-looking statements to reflect events or circumstances after the date they were made, whether as a result of new information, future events or otherwise, except as may be required under applicable securities laws.

You should not place undue reliance on these forward-looking statements in deciding how to vote your proxy or instruct how your vote should be cast on the proposals set forth in this proxy statement/prospectus. As a result of a number of known and unknown risks and uncertainties, our actual results or performance may be materially different from those expressed or implied by these forward-looking statements. Some factors that could cause actual results to differ include:

- the occurrence of any event, change or other circumstances that could delay the Business Combination or give rise to the termination of the Merger Agreement;
- the outcome of any legal proceedings that may be instituted against LGL or IronNet following announcement of the proposed Business Combination and transactions contemplated thereby;
- the inability to complete the Business Combination due to the failure to obtain approval of the stockholders of LGL or to satisfy other conditions to the closing of the proposed Merger in the Business Combination Agreement;
- the ability to obtain or maintain the listing of LGL's securities on the NYSE following the Business Combination;
- the risk that the proposed Business Combination disrupts current plans and operations of IronNet as a result of the consummation of the transactions described herein;
- the potential liquidity and trading of LGL's public securities;
- the inability to recognize the anticipated benefits of the proposed Business Combination, which may be affected by, among other things, the amount of cash available following any redemption of public shares by LGL stockholders;
- the ability of the Combined Company to execute its business model and operate in highly competitive markets, and potential adverse effects of this competition;
- risk of decreased revenues due to pricing pressures;
- the Combined Company's ability to attract, motivate and retain qualified employees, including members of its senior management team;
- the Combined Company's ability to maintain a high level of client service and expand operations;
- potential failure to comply with privacy and information security regulations governing the client datasets IronNet processes and stores;
- the risk that IronNet or the Combined Company is unsuccessful in integrating potential acquired businesses and product lines;
- potential issues with IronNet's product offerings that could cause legal exposure, reputational damage and an inability to deliver products or services;
- the ability of the Combined Company to develop new products, improve existing products and adapt its business model to keep pace with industry trends;
- the risk that IronNet's products and services fail to interoperate with third-party systems;
- the ability to maintain effective controls over disclosure and financial reporting that enable the Combined Company to comply with regulations and produce accurate financial statements;

Table of Contents

- the potential disruption of IronNet’s products, offerings, website and networks;
- the ability to deliver products and services following a disaster or business continuity event;
- increased risks resulting from IronNet’s international operations;
- potential unauthorized use of IronNet’s products and technology by third parties;
- global economic conditions;
- the impact of health epidemics, including the COVID-19 pandemic, on IronNet’s business and the actions IronNet or the Combined Company may take in response thereto;
- exchange rate fluctuations and volatility in global currency markets;
- changes in applicable laws or regulations;
- the ability to comply with various trade restrictions, such as sanctions and export controls;
- potential intellectual property infringement claims;
- the ability to comply with the anti-corruption laws of the United States and various international jurisdictions;
- potential impairment charges related to goodwill, identified intangible assets and fixed assets;
- potential litigation involving LGL or IronNet following the consummation of the Business Combination;
- costs related to the Business Combination;
- the Combined Company’s ability to raise capital; and
- other risks and uncertainties indicated in this proxy statement/prospectus, including those set forth under the section entitled “*Risk Factors*.”

Before you grant your proxy or instruct your bank or broker how to vote, or vote on the Business Combination proposal, the LGL charter proposals, the NYSE proposal, the director election proposal, the incentive plan proposal, the ESPP proposal or the adjournment proposal, you should be aware that the occurrence of the events described in the section entitled “*Risk Factors*” and elsewhere in this proxy statement/prospectus may adversely affect LGL and/or IronNet.

[Table of Contents](#)**RISK FACTORS**

The Combined Company will face a market environment that cannot be predicted and that involves significant risks, many of which will be beyond its control. In addition to the other information contained in this proxy statement/prospectus, stockholders should carefully consider the following risk factors, together with all of the other information included in this proxy statement/prospectus, before they decide whether to vote or instruct their vote to be cast to approve the proposals described in this proxy statement/prospectus.

The value of your investment in the Combined Company following consummation of the Business Combination will be subject to the significant risks affecting IronNet and inherent to the industry in which it operates. You should carefully consider the risks and uncertainties described below and other information included in this proxy statement/prospectus. If any of the events described below occur, the Combined Company's business and financial results could be adversely affected in a material way. This could cause the trading price of its common stock to decline, perhaps significantly, and you therefore may lose all or part of your investment.

Risks Related to IronNet's Business and Industry

IronNet has experienced rapid growth in recent periods, and if the Combined Company does not manage its future growth, its business and results of operations will be adversely affected.

IronNet has experienced rapid revenue growth in recent periods, and following the Business Combination the Combined Company expects to continue to invest broadly across its organization to support its growth. For example, IronNet's headcount grew from 196 full-time employees as of January 31, 2019 to 246 full-time employees as of January 31, 2021 and 296 full-time employees as of July 31, 2021. Although IronNet has experienced rapid growth historically, following the Business Combination, the Combined Company may not be able sustain IronNet's current growth rates, nor can we assure you that the Combined Company's investments to support its growth will be successful. The growth and expansion of the Combined Company's business will require it to invest significant financial and operational resources and the continuous dedication of its management team. IronNet has encountered, and the Combined Company will continue to encounter, risks and difficulties frequently experienced by rapidly growing companies in evolving industries, including market acceptance of its products, adding new customers, intense competition, and its ability to manage its costs and operating expenses. The Combined Company's future success will depend in part on its ability to manage its growth effectively, which will require the Combined Company to, among other things:

- effectively attract, integrate and retain a large number of new employees, particularly members of its sales and marketing, data science, and research and development teams;
- further improve its platform and products, including its cloud modules and security capabilities, analytics, collective defense capabilities, and visualizations, and IT infrastructure, including expanding and optimizing its data centers, collection, and analytic capabilities, to support its business needs;
- enhance its information and communication systems to ensure that its employees and offices around the world are well coordinated and can effectively communicate with each other and its growing base of customers and partners; and
- improve its financial, management, and compliance systems and controls.

If the Combined Company fails to achieve these objectives effectively, its ability to manage its expected growth, ensure uninterrupted operation of its platform and key business systems, and comply with the rules and regulations applicable to its business could be impaired. Additionally, the quality of its platform and services could suffer and it may not be able to adequately address competitive challenges. Any of the foregoing could adversely affect the Combined Company's business, results of operations, and financial condition.

[Table of Contents](#)***IronNet has a history of losses and the Combined Company may not be able to achieve or sustain profitability in the future.***

IronNet has incurred net losses in all periods since its inception. IronNet experienced net losses of \$55.4 million and \$47.9 million for fiscal 2021 and fiscal 2020, respectively, and \$15.5 million and \$16.4 million for the three months ended April 30, 2021 and 2020, respectively. As of April 30, 2021, IronNet had an accumulated deficit of \$188.8 million. While IronNet has experienced significant growth in revenue in recent periods, we cannot predict when or whether the Combined Company will reach or maintain profitability. We also expect the Combined Company's operating expenses to increase over IronNet's historical expenses in the future as the Combined Company continues to invest for future growth, which will negatively affect its results of operations if its total revenue does not increase. We cannot assure you that these investments will result in substantial increases in its total revenue or improvements in its results of operations. In addition to the anticipated costs to grow the Combined Company's business, we also expect to incur significant additional legal, accounting, and other expenses as a newly public operating company. Any failure to increase the Combined Company's revenue as it invests in its business or to manage its costs could prevent it from achieving or maintaining profitability or positive cash flow.

IronNet's limited operating history makes it difficult to evaluate its current business and the Combined Company's future prospects and may increase the risk of your investment.

IronNet was founded in 2014 and launched its first cybersecurity network detection and response product in 2016 (IronDefense) and its first collective defense product in 2018 (IronDome). IronNet's limited operating history makes it difficult to evaluate its current business, the Combined Company's future prospects, and other trends, including its ability to plan for and model future growth. IronNet has encountered, and the Combined Company will continue to encounter, risks, uncertainties, and difficulties frequently experienced by rapidly growing companies in evolving industries, including its ability to achieve broad market acceptance of cloud-enabled, and/or software as a service ("SaaS") delivered cybersecurity solutions and its platform, attract additional customers, grow partnerships, compete effectively, build and maintain effective compliance programs, and manage increasing expenses as it continues to invest in its business. If the Combined Company does not address these risks, uncertainties and difficulties successfully, its business, and results of operations will be harmed. Further, IronNet has limited historical financial data and operates in a rapidly evolving market. As a result, any predictions about the Combined Company's future revenue and expenses may not be as accurate as they would be if IronNet had a longer operating history or operated in a more predictable market.

The COVID-19 pandemic could adversely affect the Combined Company's business, operating results and future revenue.

In March 2020, the World Health Organization declared COVID-19 a global pandemic. This contagious disease outbreak has spread across the globe and is impacting worldwide economic activity and financial markets. In light of the uncertain and rapidly evolving situation relating to the spread of COVID-19, IronNet has taken precautionary measures intended to mitigate the spread of the virus and minimize the risk to its employees, customers, partners, and the communities in which it operates. These measures include transitioning its employee population to work remotely from home, imposing travel restrictions for its employees, shifting customer, partner and investor events to virtual-only formats, and limiting capacity at any of its offices which have reopened or may reopen during the pandemic's duration. These precautionary measures, many of which IronNet has now made largely permanent and sustainable, and associated economic issues, both in the United States and across the globe, could negatively affect IronNet's CS efforts, significantly delay and lengthen its sales cycles, impact its sales and marketing efforts, reduce employee efficiency and productivity, slow its international expansion efforts, increase cybersecurity risks, and create operational or other challenges, any of which could harm its business and results of operations. Moreover, due to IronNet's subscription-based business model, the effect of the COVID-19 pandemic may not be fully reflected in the Combined Company's results of operations until future periods, if at all.

[Table of Contents](#)***If IronNet's customers do not renew their subscriptions for its products, the Combined Company's future results of operations could be harmed.***

In order for the Combined Company to maintain or improve its results of operations, it is important that IronNet's customers renew their subscriptions for its platform and solutions when existing contract terms expire, and that the Combined Company expands its commercial relationships with IronNet's existing customers by selling additional subscriptions. IronNet's customers have no obligation to renew their subscriptions after the expiration of their contractual subscription period, which is generally one year, and in the normal course of business, some customers have elected not to renew. In addition, IronNet's customers may renew for shorter contract subscription lengths or cease using certain solutions. IronNet's customer retention and expansion may decline or fluctuate as a result of a number of factors, including its customers' satisfaction with its services, its pricing, customer security and networking issues and requirements, its customers' spending levels, mergers and acquisitions involving its customers, industry developments, competition and general economic conditions. If the Combined Company's efforts to maintain and expand its relationships with IronNet's existing customers are not successful, the Combined Company's business, results of operations, and financial condition may materially suffer.

As a first mover in collective defense for the commercial sector, IronNet may face significant liability if it is unable to effectively anonymize and safeguard its clients' data.

IronNet is the first major commercial vendor to offer an end-to-end means to take full advantage of the collective defense concept that relies on customers sharing sensitive customer information with IronNet. While raw customer information is not shared with other parties and shared data undergoes filtering and other transformations within the IronNet solution, with the goal of removing any sensitive or personal information, it is possible that customer information could be accessed by third parties (including competitors of IronNet's clients), through a failure of IronNet's procedures to effectively anonymize the shared data or as a result of hackers gaining access to the raw data collected by IronNet. To the extent IronNet is not able to effectively anonymize and protect its customers' data, it may be subject to liability, which could adversely affect its business, results of operations and financial condition. In addition, given the novelty of IronNet's approach, it is possible that other risks could surface of which IronNet is currently unaware.

Competition from existing or new companies could cause IronNet to experience downward pressure on prices, fewer customer orders, reduced margins, the inability to take advantage of new business opportunities and loss of market share.

The market for cybersecurity solutions is intensely competitive, fragmented, and characterized by rapid changes in technology, customer requirements, industry standards, increasingly sophisticated attackers, and by frequent introductions of new or improved products to combat security threats. We expect the Combined Company to continue to face intense competition from IronNet's current competitors, as well as from new entrants into the market. If the Combined Company is unable to anticipate or react to these challenges, its competitive position could weaken, and it could experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect its business, financial condition and results of operations. The ability to compete effectively will depend upon numerous factors, many of which are beyond IronNet's control, including, but not limited to:

- product capabilities, including performance and reliability, of its platform, including its services and features particularly in the areas of analytics and collective defense, compared to those of its competitors;
- its ability, and the ability of its competitors, to improve existing products, services and features, or to develop new ones to address evolving customer needs;
- its ability to attract, retain and motivate talented employees;

Table of Contents

- its ability to establish, capitalize on, maintain, and grow relationships with distribution and technology partners;
- the strength of its sales and marketing efforts; and
- acquisitions or consolidation within its industry, which may result in more formidable competitors.

IronNet's competitors include the following companies by general category:

- First generation Network Detection and Response (NDR) vendors such as DarkTrace or Vectra Networks, who offer point products based on Bayesian analysis, outlier analysis, and heuristic detection-based detection;
- Network security vendors, such as Cisco and Palo Alto Networks, Inc., who are supplementing their core network security additional behavioral-based detection with behavioral-based detection, threat intelligence and security operations solutions; and
- Legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products.

Many of these competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a significantly larger base of customers than IronNet does. They may be able to devote greater resources to the development, promotion, and sale of services than the Combined Company can, and they may offer lower pricing than IronNet does. Further, they may have greater resources for research and development of new technologies, the provision of customer support, and the pursuit of acquisitions, or they may have other financial, technical or other resource advantages. IronNet's larger competitors have substantially broader and more diverse product and services offerings as well as routes to market, which may allow them to leverage their relationships based on other products, or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing IronNet's products.

Conditions in IronNet's market could change rapidly and significantly as a result of technological advancements, partnering or acquisitions by competitors or continuing market consolidation. Some of IronNet's current or potential competitors have made or could make acquisitions of businesses or establish cooperative relationships that may allow them to offer more directly competitive and comprehensive solutions than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in the market or the Combined Company's failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, increased net losses and loss of market share. Further, many competitors that specialize in providing protection from particular types of security threats may be able to deliver these more targeted security products to the market quicker than the Combined Company can or may be able to convince organizations that these more limited products meet their needs.

Even if there is significant demand for cloud-based security solutions like IronNet's or if its competitors include functionality that is, or is perceived to be, equivalent to or better than IronNet's in legacy products that are already generally accepted as necessary components of an organization's cybersecurity architecture, the Combined Company may have difficulty increasing the market penetration of IronNet's platform. Furthermore, even if the functionality offered by other security and IT operations providers is different and more limited than the functionality of IronNet's platform, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like IronNet. If the Combined Company is unable to compete successfully, its business, financial condition, and results of operations would be adversely affected.

Competitive pricing pressure may reduce gross profits and adversely affect the Combined Company's financial results.

If the Combined Company is unable to maintain IronNet's pricing due to competitive pressures or other factors, its margins may be reduced and its gross profits, business, results of operations and financial condition

Table of Contents

If IronNet does not effectively expand and train its direct sales force, it may be unable to add new customers or increase sales to existing customers, and its business will be adversely affected.

IronNet depends on its direct sales force to obtain new customers and increase sales with existing customers. Its ability to achieve significant revenue growth will depend, in large part, on its success in recruiting, training and retaining sufficient numbers of sales personnel, particularly in international markets. IronNet has expanded its sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that IronNet requires. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by IronNet's long sales cycles. IronNet's recent hires and planned hires may not become productive as quickly as it expects, and the Combined Company may be unable to hire or retain sufficient numbers of qualified individuals in the markets where IronNet does business or plans to do business. In addition, a large percentage of IronNet's salesforce is new to its business and selling its solutions, and therefore this team may be less effective than its more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding its existing presence, requires upfront and ongoing expenditures that IronNet may not recover if the sales personnel fail to achieve full productivity. We cannot predict whether, or to what extent, the Combined Company's sales will increase as it expands its sales force or how long it will take for sales personnel to become productive. If the Combined Company is unable to hire and train a sufficient number of effective sales personnel, or the sales personnel it hires are not successful in obtaining new customers or increasing sales to IronNet's existing customer base, the Combined Company's business and results of operations will be adversely affected.

Because IronNet recognizes revenue from subscriptions to its platform and other forms of providing customers with access to its software over the term of the subscription or contract, downturns or upturns in new business will not be immediately reflected in the Combined Company's results of operations.

IronNet generally recognizes revenue from customers ratably over the terms of their subscription or contract term, which average over three years in length, though may be as short as one year or less. As a result, a substantial portion of the revenue that IronNet reports in each period is attributable to the recognition of deferred revenue relating to agreements that it entered into during previous periods. Consequently, any increase or decline in new sales or renewals in any one period will not be immediately reflected in its revenue for that period. Any such change, however, would affect its revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in IronNet's rate of renewals may not be fully reflected in the Combined Company's results of operations until future periods.

A limited number of customers represent a substantial portion of IronNet's revenue. If the Combined Company fails to retain these customers, its revenue could decline significantly.

IronNet derives a substantial portion of its revenue from a limited number of customers. For fiscal 2021 and fiscal 2020, six customers accounted for 46% and four customers accounted for 48% of IronNet's revenues, respectively. As of April 30, 2021 and 2020, two and four customers represented 94% and 84%, respectively, of IronNet's total accounts receivable balance. Significant customers are those which represent at least 10% of IronNet's total revenue at each respective period ending date. The following table presents customers that represent 10% or more of IronNet's total annual revenue:

	<u>Year Ended January 31,</u>	
	<u>2021</u>	<u>2020</u>
Customer A	10%	*
Customer B	*	14%
Customer C	*	10%
Customer D	*	10%
Customer E	*	14%

* Less than 10%

For the quarter ended April 30, 2021, three significant customers accounted for 32% of IronNet's revenues.

Table of Contents

As a result, the Combined Company's revenue could fluctuate materially and could be materially and disproportionately impacted by purchasing decisions of these customers or any other significant future customer. Any of the Combined Company's significant customers may decide to purchase less than they have in the past, may alter their purchasing patterns at any time with limited notice, or may decide not to continue to license IronNet's products at all, any of which could cause the Combined Company's revenue to decline and adversely affect its financial condition and results of operations. If the Combined Company does not further diversify IronNet's customer base, it will continue to be susceptible to risks associated with customer concentration.

IronNet's results of operations may fluctuate significantly, which could make its future results difficult to predict and could cause its results of operations to fall below expectations.

IronNet's results of operations have varied significantly from period to period, and we expect that the Combined Company's results of operations will continue to vary as a result of a number of factors, many of which are outside of IronNet's control and may be difficult to predict, including:

- the impact of the COVID-19 pandemic on its operations, financial results, and liquidity and capital resources, including on customers, sales, expenses, and employees;
- its ability to attract new and retain existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;
- the timing and length of its sales cycles;
- changes in customer or distribution partner requirements or market needs;
- changes in the growth rate of its market;
- the timing and success of new product and service introductions by it or its competitors or any other competitive developments, including consolidation among its customers or competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of its platform;
- its ability to successfully expand its business domestically and internationally;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in its pricing policies or those of its competitors;
- any disruption in its relationship with distribution partners;
- insolvency or credit difficulties confronting its customers, affecting their ability to purchase or pay for its solutions;
- significant security breaches of, technical difficulties with or interruptions to, the use of its platform;
- extraordinary expenses such as litigation or other dispute-related settlement payments or outcomes;
- general economic conditions, both in domestic and foreign markets;
- future accounting pronouncements or changes in its accounting policies or practices;
- negative media coverage or publicity;
- political events;
- the amount and timing of operating costs and capital expenditures related to the expansion of its business; and
- increases or decreases in expenses caused by fluctuations in foreign currency exchange rates.

In addition, IronNet experiences seasonal fluctuations in its financial results as it can receive a higher percentage of its annual orders from new customers, as well as renewal orders from existing customers, in the

Table of Contents

fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of its customers. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in the Combined Company's financial and other results from period to period. As a result of this variability, IronNet's historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in the Combined Company's failure to meet its operating plan or the expectations of investors or analysts for any period. If it fails to meet such expectations for these or other reasons, the Combined Company's stock price could fall substantially, and it could face costly lawsuits, including securities class action suits.

IronNet's sales cycles can be long and unpredictable, and its sales efforts require considerable time and expense.

IronNet's revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for its platform, particularly with respect to large organizations and government entities. Customers often view the subscription to its platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test, and qualify its platform and solutions prior to entering into or expanding a relationship with it. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens its sales cycle.

IronNet's direct sales team develops relationships with its customers, and works with its distribution partners on account penetration, account coordination, sales and overall market development. IronNet spends substantial time and resources on its sales efforts without any assurance that its efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals, and unanticipated administrative, processing, and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of IronNet's efforts to secure sales after investing resources in a lengthy sales process could adversely affect its business and results of operations.

IronNet relies heavily on the services of its senior management team, and if the Combined Company is not successful in attracting or retaining senior management personnel, it may not be able to successfully implement IronNet's business strategy.

The Combined Company's future success will be substantially dependent on its ability to attract, retain, and motivate the members of its management team. In particular, the Combined Company will be highly dependent on the services of Gen. Keith B. Alexander (Ret.) and William Welch, the co-chief executive officers of the Combined Company, who will be critical to its future vision and strategic direction. It will also rely on its leadership team in the areas of operations, security, analytics, engineering, product management, research and development, marketing, sales, partnerships, mergers and acquisitions, support, and general and administrative functions. Gen. Keith B. Alexander (Ret.) is important to IronNet's future growth as he provides access to key decisionmakers within government agencies and the private sector, and his leadership role at the Combined Company would be difficult to replace. Although we expect that the Combined Company will enter into employment agreements with its key personnel following the consummation of the Business Combination, its employees, including its executive officers, will be employed on an "at-will" basis, which means they may terminate their employment with the Combined Company at any time. If one or more of the Combined Company's key employees resigns or otherwise ceases to provide it with their service, its business could be harmed.

If the Combined Company is unable to attract and retain qualified personnel, its business could be harmed.

There is significant competition for personnel with the skills and technical knowledge that the Combined Company will require across its technology, cyber, sales, professional services and administrative support functions. Competition for these personnel in the Washington, D.C. metro area, where the corporate headquarters of the Combined Company will be located, and in other locations where it maintains offices or otherwise

Table of Contents

If the Combined Company is unable to maintain successful relationships with IronNet's distribution partners, or if its distribution partners fail to perform, the Combined Company's ability to market, sell and distribute IronNet's platform and solutions efficiently will be limited, and its business, financial position and results of operations will be harmed.

In addition to its direct sales force, IronNet relies on certain key distribution partners to sell and support its platform. An increasing amount of IronNet's sales flow through its distribution partners, and IronNet expects its reliance on such partners to continue to grow for the foreseeable future. Additionally, IronNet has entered into, and the Combined Company intends to continue to enter into, partnerships with third parties to support its future growth plans. The loss of a substantial number of distribution partners, or the failure to recruit additional partners, could adversely affect the Combined Company's results of operations. The Combined Company's ability to achieve revenue growth in the future will depend in part on its success in maintaining successful relationships with IronNet's distribution partners and in training them to independently sell and deploy IronNet's platform. If the Combined Company fails to effectively manage IronNet's existing sales channels, or if IronNet's distribution partners are unsuccessful in fulfilling the orders for its solutions, or if the Combined Company is unable to recruit and retain a sufficient number of high quality distribution partners who are motivated to sell IronNet's products, the Combined Company's ability to sell its products and results of operations will be harmed.

IronNet's business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on the Combined Company's business and results of operations.

IronNet's future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable, subject to budgetary uncertainty and typically involves long sales cycles. IronNet has made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that the Combined Company will be able to maintain or grow its revenue from the government sector. Although we anticipate that they may increase in the future, sales to U.S. federal, state and local governmental agencies have not accounted for, and may never account for, a significant portion of the Combined Company's revenue. U.S. federal, state and local government sales are subject to a number of challenges and risks that may adversely impact the Combined Company's business. Sales to such government entities include the following risks:

- selling to governmental agencies can be highly competitive, expensive and time-consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- government certification requirements applicable to IronNet's products may change and, in doing so, restrict the Combined Company's ability to sell into the U.S. federal government sector until it has attained the required certifications.
- government demand and payment for IronNet's platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for its platform;
- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying IronNet's platform, which would adversely impact the Combined Company's revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities;
- interactions with the U.S. federal government may be limited by post-employment ethics restrictions on members of IronNet's management;
- foreign governments may have concerns with purchasing security products from a company that employs former NSA employees and officials, which may negatively impact sales; and
- governments may require certain products to be manufactured, hosted, or accessed solely in their country or in other relatively high-cost manufacturing locations, and the Combined Company may not

Table of Contents

manufacture all products in locations that meet these requirements, affecting its ability to sell these products to governmental agencies.

IronNet has achieved Federal Risk and Authorization Management Program (“FedRAMP”) “FedRAMP-ready” status, but such status is only available for a certain period of time before which it must be utilized. If not utilized, IronNet would likely have to go through certain parts of the FedRAMP process again in order to sell its products to government agencies. Moreover, even if IronNet were to achieve FedRAMP-certified status, such certification is costly to maintain, and if the Combined Company were to lose such a certification in the future it would restrict its ability to sell to government customers. It is also possible that additional guidelines and/or certifications, such as the Cybersecurity Maturity Model Certification (“CMMC”), will be required to expand participation in the government sectors.

The occurrence of any of the foregoing could cause governments and governmental agencies to delay or refrain from purchasing IronNet’s solutions in the future or otherwise have an adverse effect on the Combined Company’s business and results of operations.

The Combined Company may not scale and adapt IronNet’s existing technology in a timely and cost-effective manner to meet its customers’ performance and other requirements.

The Combined Company’s future growth will be dependent upon its ability to continue to meet the needs of new customers and the expanding needs of IronNet’s existing customers as their use of its solutions grows. As IronNet’s customers gain more experience with its solutions, the number of events, the amount of data transferred, processed, and stored by it, the number of locations where its platform and services are being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of IronNet’s customers, the Combined Company intends to continue to make significant investments to increase capacity and to develop and implement new technologies in its service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new, and untested. The Combined Company may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop, and test improvements to IronNet’s technologies and infrastructure, and the Combined Company may not be able to accurately forecast demand or predict the results it will realize from such improvements. To the extent that the Combined Company does not effectively scale IronNet’s operations to meet the needs of its growing customer base and to maintain performance as its customers expand their use of its solutions, the Combined Company may not be able to grow as quickly as anticipated, customers may reduce or cancel use of IronNet’s solutions and the Combined Company may be unable to compete as effectively and its business and results of operations may be harmed.

Additionally, IronNet has made, and the Combined Company will continue to make, substantial investments to support growth at its data centers partners and improve the profitability of its cloud platform. If the Combined Company’s cloud-based server costs were to increase or pricing pressure causes price movements out of proportion with changes in unit operating costs, its business, results of operations and financial condition may be adversely affected. Although we expect that the Combined Company could receive similar services from other third parties, if any of IronNet’s arrangements with third-party providers are terminated, IronNet could experience interruptions on its platform and in its ability to make its solutions available to customers, as well as delays and additional expenses in arranging alternative cloud infrastructure services. Ongoing improvements to cloud infrastructure may be more expensive than anticipated and may not yield the expected savings in operating costs or the expected performance benefits. In addition, the Combined Company may be required to re-invest any cost savings achieved from IronNet’s prior cloud infrastructure improvements in future infrastructure projects to maintain the levels of service required by its customers. The Combined Company may not be able to maintain or achieve cost savings from its investments, which could harm its financial results.

[Table of Contents](#)

that are not emerging growth companies. If some investors find the Combined Company Common Stock less attractive as a result, there may be a less active trading market for the Combined Company Common Stock, and the market price of the Combined Company Common Stock may be more volatile.

IronNet's management has limited experience in operating a public company.

IronNet's executive officers have limited experience in the management of a publicly traded company. IronNet's management team may not successfully or effectively manage its transition to a public company that will be subject to significant regulatory oversight and reporting obligations under federal securities laws. Their limited experience in dealing with the increasingly complex laws pertaining to public companies could be a significant disadvantage in that it is likely that an increasing amount of their time may be devoted to these activities, which will result in less time being devoted to the management and growth of the Combined Company. IronNet may not have adequate personnel with the appropriate level of knowledge, experience, and training in the accounting policies, practices or internal control over financial reporting required of public companies in the United States. The development and implementation of the standards and controls necessary for the Combined Company to achieve the level of accounting standards required of a public company in the United States may require costs greater than expected. It is possible that the Combined Company will be required to expand its employee base and hire additional employees to support its operations as a public company, which will increase its operating costs in future periods.

If securities or industry analysts do not publish research or reports about the Combined Company's business or publish negative reports, the market price of its common stock could decline.

The trading market for the Combined Company Common Stock will be influenced by the research and reports that industry or securities analysts publish about the Combined Company or its business. If regular publication of research reports ceases, the Combined Company could lose visibility in the financial markets, which in turn could cause the market price or trading volume of the Combined Company Common Stock to decline. Moreover, if one or more of the analysts who cover the Combined Company downgrade its common stock or if reporting results do not meet their expectations, the market price of the common stock could decline.

A significant portion of Combined Company Common Stock following the Business Combination will be restricted from immediate resale, but may be sold into the market in the future. Future sales could cause the market price of Combined Company Common Stock to drop significantly, even if the Combined Company's business is doing well.

After the Business Combination, it is anticipated that there will be outstanding (i) approximately 100,000,000 shares of Combined Company Common Stock (assuming that no shares of LGL common stock redeemed by LGL stockholders), (ii) warrants to purchase approximately 13,825,000 shares of Combined Company Common Stock and (iii) assumed IronNet options and restricted stock units covering approximately 19,000,000 shares of Combined Company Common Stock.

Pursuant to lock-up agreements (the "*IronNet Lock-Up Agreement*") entered into by and among LGL and certain stockholders and employees of IronNet signatories thereto, including IronNet's executive officers, directors and 5% stockholders (the "*IronNet Lock-Up Parties*"), who will hold in the aggregate approximately 66 million shares of LGL common stock upon consummation of the Business Combination, the IronNet Lock-Up Parties have agreed that, with respect to LGL common stock, through the date that is 180 days after the closing of the Business Combination, and, with respect to LGL warrants and any LGL common stock issuable upon the exercise of LGL warrants, through the date that is 30 days after the closing of the Business Combination, subject to certain exceptions, to not, without the prior written consent of the LGL board of directors, among other things, sell, offer to sell, contract or agree to sell, hypothecate, pledge, grant any option to purchase or otherwise dispose of or agree to dispose of, directly or indirectly any shares of LGL common stock, LGL warrants LGL common

Table of Contents

stock issuable upon the exercise of LGL warrants, as applicable, held by the IronNet Lock-Up Parties; *provided, however*, certain founders and employees of IronNet, including an executive officer, have been granted relief from the lock-up to sell up to an aggregate of approximately 1.5 million shares of LGL common stock, and these shares will be eligible for sale immediately after consummation of the Business Combination, subject to compliance with applicable securities laws. In addition, pursuant to the Sponsor Agreement, as amended by Sponsor Agreement Amendment (and similar agreements entered into by all of LGL's executive officers and directors), the Sponsor and LGL's executive officers and directors have agreed, subject to certain exceptions, to not transfer, assign or sell the 3,234,375 shares of Combined Company Common Stock to be received upon conversion of the Sponsor's remaining Founder Shares (after the forfeiture of 1,078,125 Founder Shares pursuant to the Sponsor Support Agreement) (the "*Remaining Founder Shares*") until six months after the closing of the Business Combination and to not transfer, assign or sell the Private Warrants or any LGL common stock issuable upon exercise of the Private Warrants until 30 days after the closing of the Business Combination.

However, following the expiration of such lock-up periods, these lock-up parties will not be restricted from selling Combined Company securities held by them, other than by applicable securities laws. Additionally, the Subscription Investors will not be restricted from selling any of their shares of Combined Company Common Stock after the closing of the Business Combination, other than by applicable securities laws.

In connection with the Business Combination, LGL's existing registration rights agreement will be amended and restated to: (i) provide that the Combined Company will file a shelf registration statement 30 days following the closing of the Business Combination to register for resale under the Securities Act of (A) all LGL securities held by the Sponsor at the time the Registration Rights Agreement is entered into, including the 3,234,375 shares of Combined Company Common Stock to be received upon conversion of the Remaining Founder Shares, the 566,000 shares of LGL common stock issued to the Sponsor in the Private Placement, the Private Warrants and shares of LGL common stock issuable upon exercise of the Private Warrants held by the Sponsor, and (B) certain of the shares of the Combined Company Common Stock to be issued to IronNet stockholders in the Business Combination, including IronNet's executive officers, directors and greater than 5% stockholders and (ii) afford each such party "piggyback" registration rights with respect to any underwritten offerings by the other stockholders and by the Combined Company. In addition, pursuant to the Subscription Agreements, LGL has agreed to file a shelf registration statement within 30 days following the closing of the Business Combination to register the resale under the Securities Act of the shares of LGL common stock purchased by the Subscription Investors.

Sales of a substantial number of shares of Combined Company Common Stock in the public market could occur at any time, particularly after expiration of the above-mentioned lock-up periods and the registration of the resale of the Combined Company securities discussed above. These sales, or the perception in the market that the members of management of the Combined Company or holders of a large number of shares intend to sell shares, could reduce the market price of Combined Company Common Stock and the LGL warrants.

The Combined Company has no current plans to pay cash dividends on its common stock. As a result, stockholders may not receive any return on investment unless they sell their common stock for a price greater than the purchase price.

The Combined Company has no current plans to pay dividends on its common stock. Any future determination to pay dividends will be made at the discretion of the Combined Company Board, subject to applicable laws. It will depend on a number of factors, including the Combined Company's financial condition, results of operations, capital requirements, contractual, legal, tax and regulatory restrictions, general business conditions, and other factors that the Combined Company Board may deem relevant. In addition, the ability to pay cash dividends may be restricted by the terms of debt financing arrangements, as any future debt financing arrangement likely will contain terms restricting or limiting the amount of dividends that may be declared or paid on the common stock. As a result, stockholders may not receive any return on an investment in the Combined Company Common Stock unless they sell their shares for a price greater than that which they paid for them.

[Table of Contents](#)**THE MERGER AGREEMENT**

For a discussion of the structure of the transactions and consideration, see the section entitled “*Proposal No. 1—The Business Combination Proposal*.” Such discussion and the following summary of other material provisions of the Merger Agreement is qualified by reference to the complete text of the Merger Agreement, a copy of which is attached as *Annex A* to this proxy statement/prospectus. All stockholders are encouraged to read the Merger Agreement in its entirety for a more complete description of the terms and conditions of the transactions.

On March 15, 2021, LGL entered into a merger agreement by and among LGL, Merger Sub and IronNet, which subsequently was amended on August 6, 2021. Pursuant to the Merger Agreement, Merger Sub will merge with and into IronNet, with IronNet surviving the merger. As a result of the Business Combination, IronNet will become a wholly-owned subsidiary of LGL, with the stockholders of IronNet becoming stockholders of LGL.

Pursuant to the Merger Agreement, (i) each outstanding share of IronNet common stock and IronNet preferred stock (with each share of IronNet preferred stock being treated as if it were converted into ten (10) shares of IronNet common stock on the effective date of the Business Combination) will be converted into the right to receive (a) a number of share of LGL common stock equal to the Exchange Ratio and (b) a cash amount payable in respect of fractional shares of LGL common stock that would otherwise be issued in connection with the foregoing conversion, if applicable, and (ii) each IronNet option, IronNet restricted stock unit, IronNet restricted stock award or IronNet warrant that is outstanding immediately prior to the closing of the transactions (and by its terms will not terminate upon the closing of the transactions) will remain outstanding and thereafter (x) in the case of options, represent the right to purchase a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such option multiplied by the Exchange Ratio used for IronNet common stock (rounded down to the nearest whole share) at an exercise price per share equal to the current exercise price per share for such option divided by the Exchange Ratio (rounded up to the nearest whole cent), (y) in the case of warrants, represent the right to purchase a number of shares of LGL common stock equal to the number of shares of IronNet preferred stock subject to such warrant multiplied by Exchange Ratio, multiplied by ten at an exercise price equal to the current exercise price per share (rounded up to the nearest whole cent) for such warrant divided by the Exchange Ratio, divided by ten (10) (rounded down to the nearest whole share), and (z) in the case of stock units and restricted stock awards, represent a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such stock unit or restricted stock award multiplied by the Exchange Ratio (rounded down to the nearest whole share). In addition, IronNet stockholders and eligible holders of options, warrants, restricted stock unit awards and restricted stock awards (as applicable, only to the extent time vested as of the closing of the Business Combination) may also receive as additional merger consideration in the form of a pro rata portion of 1,078,125 shares of LGL common stock if the volume weighted average share price for LGL’s common stock equals or exceeds \$13.00 for ten (10) consecutive days during the two year period following the closing of the Business Combination.

If calculated based on the capitalization of IronNet as of July 31, 2021, the Exchange Ratio is approximately 0.8128 of a share of LGL common stock per fully-diluted share of IronNet common stock.

At the closing of the Business Combination, certain IronNet stockholders and other parties thereto will enter into the Registration Rights Agreement pursuant to which LGL agreed to file a shelf registration statement with respect to the registrable securities under the Registration Rights Agreement. LGL also agreed to provide customary “piggyback” registration rights. The Registration Rights Agreement also provides that LGL will pay certain expenses relating to such registrations and indemnify the stockholders against certain liabilities.

Certain IronNet stockholders receiving shares of LGL common stock in connection with the Business Combination will be subject to a 180-day lockup period for all shares of LGL common stock held by such persons, subject to customary carve-outs; provided, however, certain founders and employees, including an executive officer, have been granted relief from the lock-up to sell up to an aggregate of approximately 1.5 million shares of Combined Company Common Stock.

[Table of Contents](#)

INFORMATION ABOUT IRONNET

Unless the context otherwise requires, all references in this section to “IronNet” refer to IronNet Cybersecurity, Inc. and its subsidiaries prior to the consummation of the Business Combination.

The IronNet Mission: A Summary

IronNet is transforming cybersecurity through Collective Defense using its behavioral analytics technology.

IronNet competes in the Network Detection and Response (NDR) category, which is a growing aspect of modern enterprise security, but which does include major competitors. IronNet’s value proposition and competitive differentiator is its collective defense concept. IronNet’s founder and Co-CEO, Gen. Keith B. Alexander (Ret.), serves as a valuable business development resource for establishing relationships with larger enterprise and government buyers. The significant majority of IronNet’s current revenue comes from its IronDome and IronDefense products. IronDefense is an NDR cybersecurity product that uses artificial intelligence (AI), machine learning (ML), behavioral analytics, and operational tradecraft expertise to quickly identify specific network behaviors or events indicative of malicious threats. Enriched by its cyber tradecraft knowledge, alerts produced by IronNet help analysts quickly contextualize and prioritize threats that pose the greatest risks. By doing this IronNet is able to provide clients, across a variety of industries, nation-state-level defensive capabilities to reduce cyber risk.

The Cyberspace Solarium Commission suggests the importance of this service in the following statement in its March 2020 report:

“The reality is that we are dangerously insecure in cyber. Your entire life—your paycheck, your health care, your electricity—increasingly relies on networks of digital devices that store, process and analyze data. These networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state sponsored intellectual property theft using cyber espionage.”

IronNet is a metric-driven organization with a differentiated and potentially transformational approach to the cybersecurity problem facing every organization today. With an ever-increasing cybersecurity threat posed by advanced persistent threat (APT) actors, a team of experts assembled by Gen. Alexander, the longest serving Director of the National Security Agency (NSA) and Commander of Cyber Command in U.S. history, can help solve this problem. It takes knowledge of how APTs operate and their tactics, techniques and procedures in order to defeat them; few individuals and even fewer companies have that knowledge or capability. IronNet’s differentiated market offering called IronDome offers users a collective defense model to help mitigate threats posed by an APT enhanced by its IronDefense platform, offering IronNet clients new protections against an APT with its technology.

According to a report commissioned by LGL Systems to 5by5 Cyber Consulting, the question, “Does IronNet have reasonable defensive measures in place across people, processes and technology?” concluded that IronNet has invested a lot of time and effort into its security architecture, has obtained an impressive array of certifications and has undergone extensive audits and testing to ensure it is meeting industry standards. IronNet has highly skilled people in critical security roles and mature processes in place for crucial areas like change management, data protection and software development. IronNet also has a robust technology stack to defend its network and skilled analysts to operate them. IronNet takes training seriously and requires annual training for all members of the organization on information security and has a defined training track for its security analysts. While this is not a guarantee a company will not have a security breach, 5by5 concluded that IronNet has taken reasonable precautions to protect against it.

[Table of Contents](#)

Cyber Landscape Overview

“Cybersecurity is one of the most systemically important issues facing the world today. Cyber information sharing is critical to helping better collective security in the digital ecosystem in which society increasingly relies.”

— World Economic Forum

From an independent assessment of the IronNet platform performed by TAG Cyber, it is clear that cyber security has advanced from a niche technical concern to a mainstream consideration for organizations of all sizes and in all sectors. Security protection concerns are most intense where safety or life-critical consequences might arise in response to a cyber threat. Power companies, financial services firms, telecommunications companies, military organizations, and government agencies thus have the greatest need for security protection, and now make considerable investments in cyber.

The primary security challenge in modern organizations is the complexity that has evolved in the typical business or government entity. Applications, networks, systems, endpoints, and data have experienced considerable sprawl as the costs associated with computing have decreased significantly. This is especially true for cloud-based infrastructure and SaaS-based applications, where cheap ubiquitous services are now available on-demand and for nearly every purpose imaginable.

Modern organizations must therefore develop security protections that address such growth, often delivered in the context of digital transformation initiatives. An additional complication is that hackers have been augmented by determined, capable adversaries, often funded or otherwise backed by criminal groups or nation-states. Serious consideration must thus be given to the types of protections that are necessary to defend against the threat from such capable threat actors.

An additional dimension is that the velocity associated with computing infrastructure and their associated threats has accelerated. Agile DevOps processes generate new features at increasing rates, sometimes hourly for popular services, and hackers use automated platforms to bombard targeted infrastructure with alarming intensity. Security engineers thus require controls that are automated and that address this challenge of increased speed. Manually controlled point solutions no longer stop threats.

A further complication is the massive and increasing scale associated with the types of systems operated by larger enterprise teams. Large-scale IT and network systems remove the ability for organizations to rely on manual maintenance, fixed configurations, and simple asset management. Furthermore, the visibility of assets that might be well-known by smaller organizations can only be approximated in large scale settings. This greatly complicates the challenge of delivering security in a large-scale setting.

In response to these challenges, modern Chief Information Security Officers (CISOs) put considerable time and effort into designing and implementing a workable security architecture. Individual CISO-led teams – even if they focus their efforts – have come to recognize that they cannot address the cyber challenge on their own. It is well-understood in the cybersecurity community that enterprise security teams need considerable external assistance, coordination and cooperative guidance.

Some of this assistance is obvious: Businesses rarely develop their own security tools, but rather buy from vendors or adjust open-source tools. Similarly, information sharing groups have emerged to support cooperative discussions between experts. It is therefore not controversial to suggest that business and agencies need to work together to address cyber threats. The big question, instead, is how this objective can be best achieved. This is one of the challenges addressed by IronNet.

[Table of Contents](#)**Background of IronNet**

IronNet is a global cybersecurity company revolutionizing how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former National Security Agency (“NSA”) cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Gen. Alexander founded IronNet in 2014 to solve the major cybersecurity problem he witnessed and defined during his tenure as former head of the NSA and founding Commander of U.S. Cyber Command: You can’t defend against threats you can’t see. IronNet’s innovative approach provides the ability for groups of organizations—within an industry sector, supply chain, state or country, for example—to see, detect and defend against sophisticated cyber attacks earlier and faster than ever before.

IronNet has defined a new market category called Collective Defense. As the first mover in this category, IronNet has developed its Collective Defense platform, the first, and to its knowledge, the only solution that can identify anomalous (potentially suspicious or malicious) behaviors on computer networks and share this intelligence anonymously and in real time among Collective Defense community members. Collective Defense communities comprise groups of organizations that have common risks, such as a supply chain, a business ecosystem, or across an industry sector, a state, or a country. This cybersecurity model delivers timely, actionable, and contextual alerts and threat intelligence on attacks targeting enterprise networks, and functions as an early-warning detection system for all community members.

This new platform addresses a large and unwavering compound problem: limited threat visibility for increasingly borderless enterprises across sectors and at the national level, paired with ineffective threat knowledge sharing across companies and sectors and a “go it alone” approach to cybersecurity. These operational gaps, combined with market dynamics like the increased velocity of sophisticated cyber attacks and the deepening scarcity of qualified human capital, have set IronNet’s mission to transform how cybersecurity is waged.

Understanding Collective Cyber Defense

Ideally the U.S. Government could defend the nation against cyberattacks similar to what was developed for the Intercontinental Ballistic Missile (ICBM) missile threat. Unfortunately, the ability to enact such a defense would likely require limiting personal freedoms on the internet that Americans currently enjoy. Legislation limiting personal freedoms would likely be challenging to pass and thus the probability of that happening in the near future is low. The Cyberspace Solarium Commission report submitted in July 2020 contains over 80 recommendations to address the issue of cybersecurity, with one of them being “Reshaping the Cyber Ecosystem.” That report states:

“Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries’ activities. Over time this will reduce the frequency, scope, and scale of their cyber operations. Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes.”

IronNet’s collective defense model, IronDome, is a means for the private sector to “raise the baseline” level of security by partnering amongst themselves to “produce positive outcome.” This overwatch function is a differentiator for IronNet’s portfolio of offerings, making IronNet one of the few companies that has the ways, ends and means to enact this transformational concept due to the technical capabilities required to ensure its success.

[Table of Contents](#)

To properly understand the IronNet platform and solution approach, it is best to begin with an outline of how collective defense can reduce cyber risk for larger organizations. This approach benefits from many years of organizations beginning to share data through various groups such as Information Sharing and Analysis Organizations (ISAO). IronNet is the first major commercial vendor to offer an end-to-end means to take full advantage of the collective concept.

Toward a Collective Cyber Defense

Businesses and agencies will only cooperate on collective cybersecurity initiatives if they see meaningful benefits with low associated risk. Admittedly, this is how almost all business decisions are made, but large-scale cybersecurity introduces an added benefit for collective defense—namely, that cyber protection schemes work much better when they involve a wider range of intelligence, visibility, and security coverage. Working together in cybersecurity thus introduces clear benefits for participants.

Nevertheless, cooperation between businesses, agencies, and other groups must address two ends of the spectrum: upside benefits and downside risks for each of the entities and groups involved. In both instances, the case can be made that, for large-scale infrastructure, both benefits and risks can cascade, perhaps even accelerating as lateral traversal of an attack occurs. That is, threats to someone else's system, however remote, might cascade across networks and systems.

Within a large organization, collective protection across business units can have comparable benefit, particularly in companies that evolved through mergers and acquisitions, where a collective defense can help to bring together disparate data sources, defensive perspectives, and protection platforms into a common defense. Such intra-enablement within a large organization is a major focus area for IronNet.

The primary benefits of a collective defense for large-scale cyber defense, whether stretched across a sector, combined between multiple organizations, or combined across the business units of one company, include the following:

- **Early Warning System**—An organization can develop a more effective early warning system if other groups share their indicators in real-time. Not engaging in such sharing limits the ability of a local team to capitalize on early warning that a cascading attack might be underway.
- **Broader Visibility**—By working together with other groups, the local security team benefits from broader visibility, including an improved understanding of how local enterprise changes (e.g., DNS-related) might cascade to other targets.
- **Strength in Numbers**—The fact that cooperation increases visibility into a cyber threat means that organizations who cooperate with external groups are able to leverage strength-in-numbers and thereby provide better security support.

The corresponding risks that must be managed in the development of any large-scale cooperative arrangement for cybersecurity include the following:

- **Privacy of Shared Data**—The possibility emerges that sharing information with a cooperative might result in leaked data or a serious privacy incident. For highly regulated industries, sharing with government may also expose businesses to some regulatory risk (although this is partially mitigated by certain provisions of the Cybersecurity Information Security Act of 2014 (CISA)) if the data is not properly anonymized or otherwise does not comply with legal requirements. Controls must be in place to ensure that cooperating teams are not exposed to this risk.
- **Attribution of Incidents**—Public attribution of an embarrassing or problematic cybersecurity incident to a sharing entity may reduce (or even remove) the willingness of that organization (and others) to share further information about something that might reflect poorly on their own actions. This is less an issue for collective defenses implemented across the business units of one organization.

[Table of Contents](#)

- **Competitive Relationship**—The risk of one company directly assisting its competitor through participation in a collective defense scheme (e.g., AT&T assisting Verizon, or General Motors assisting Toyota) cannot be ignored. The legal and marketing teams from participating organizations would be wise to adopt the airline and energy industry’s observations that a mutual focus on safety helps every participant.

The benefits and risks of cooperation for large-scale cybersecurity across heterogeneous groups must be carefully balanced in setting up a collective defense. Too often, collectives are developed that leave participants wondering what’s in it for them, and how potential problems might be avoided. One main value proposition from IronNet is that cooperative cybersecurity will work best when such concerns are carefully curated by a trusted provider with a world-class platform.

Role of Government in Collective Defense

One challenge federal governments have in supporting collective cyber defense is that most large businesses are multi-national. This suggests that while national allegiance might be easily identified (e.g., Verizon is American, Huawei is Chinese), such allegiance must address the interests of the company’s shareholders. This emphasis is often misunderstood by government agencies who are focused exclusively on national interests.

Federal governments also have the additional role to regulate and sometimes punish organizations not meeting their security requirements. This obligation complicates government cooperation with business on cybersecurity, at least to the extent that governments are permitted to regulate based on voluntarily shared information. Organizations would thus be hesitant to share information with a cooperative involving government if the reported incident might lead to regulatory investigation.

The biggest challenge, however, is that the majority of critical infrastructure is owned and operated by the private sector. This implies that security telemetry, indicators, and early warnings will come from the private sector, even for many military applications and defensive government activities. This fact is often not understood by citizens and politicians who may demand that government step in and fix large-scale cybersecurity threats. This is usually just not practically feasible.

Government must work hard to share the information it uniquely controls, such as classified indicators that might be downgraded for sharing externally or be shared in a more limited context to defend critical infrastructure. Businesses must also recognize that their obligations extend beyond just the shareholder. This recognition that cooperative sharing is in the best interests of the organization and society in general is an important driver behind IronNet’s platform offering.

Overview of IronNet’s Platform Offering

The Collective Defense platform comprises two flagship products:

IronDefense is an advanced Network Detection and Response (“NDR”) solution that uses AI-driven behavioral analytics to detect and prioritize anomalous activity inside individual enterprises. IronNet leverages advanced Artificial Intelligence/Machine-Learning (“AI/ML”) algorithms to detect previously unknown threats that have not been identified and “fingerprinted” by industry researchers), in addition to screening any known threats, and applies its Expert System to prioritize the severity of the behaviors—all at machine speed and cloud scale.

IronDome is a threat-sharing solution that facilitates a crowdsource-like environment in which the IronDefense threat detections from an individual company are shared among members of a Collective Defense community, consisting of IronNet customers who have elected to permit their information to be anonymously shared and cross-correlated by IronNet’s IronDome systems. IronDome analyzes threat detections across the

Table of Contents

community to identify broad attack patterns and provides anonymized intelligence back to all community members in real time, giving all members early insight into potential incoming attacks. Automated sharing across the Collective Defense community enables faster detection of attacks at earlier stages.

IronNet's Collective Defense platform is designed to deliver strong network effects. Every customer contributing its threat data (anonymously) into the community is able to reap benefits from the shared intelligence of the other organizations. The collaborative aspect of Collective Defense, and the resulting prioritization of alerts based on their potential severity, helps address the known problem of "alert fatigue" that plagues overwhelmed security analysts.

The Collective Defense platform is available for on-premise, cloud (public or private), and hybrid environments, and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. IronNet provides professional cybersecurity services such as incident response and threat hunting, as well as programs to help customers assess cybersecurity governance, maturity, and readiness. IronNet's CS services are designed to create shared long-term success measures with its customers, differentiating it from other cybersecurity vendors by working alongside customers as partners and offering consultative and service capabilities beyond implementation.

The Collective Defense platform is available via a subscription-based pricing and flexible delivery model, with options available for major public cloud providers such as Amazon Web Services and Microsoft Azure; private cloud, or Hyper Converged Infrastructure ("HCP") such as Nutanix; and on-premise environments through hardware and virtual options. To make it as easy as possible for customers to add Collective Defense into their existing security stack, IronNet built a rich set of Application Programming Interfaces ("APIs") that enable integrations with standard security products, including security information and event management ("SIEM"); security orchestration, automation, and response ("SOAR"); endpoint detection and response ("EDR"); next-generation firewall ("NGFW") tools; and cloud-native logs from the major public cloud providers.

IronNet describes its go-to-market strategy as "land and expand with network effects." Its approach is to initially secure influential "cornerstone" customers and then expand into their respective Collective Defense communities with additional "community members" from organizations of similar industry sector, state, country, supply chain, or tailored business ecosystem. As each Collective Defense community grows, so does the volume of shared data, and the value of IronNet's platform for each of those members thereby expands both technically and commercially.

IronNet sells into both public and private organizations and the business ecosystems that support them. IronNet has identified tens of thousands of prospective cornerstone customers and more than 100,000 potential community customers.

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust IronNet to protect their networks. IronNet's customers include a top global hedge fund, eight of the top 10 U.S. energy companies (based on revenue), a leading Asian mobile phone carrier, two U.S. Department of Defense ("DoD") branches, a mid-sized bank in the EMEA region, four U.S. state agencies, U.K. and Singapore government entities, and a large global holding company.

IronNet began targeting large enterprises and Fortune 500 companies, but the flexibility and scalability of its cloud-native platform and enhanced go-to-market approach enabled it to expand its customer base to smaller companies as well. IronNet has been recognized in the cybersecurity industry by independent third-party analysts, including Gartner, Forrester, IDC, 451 Research Group, and Omdia, who has called IronNet's analytics a "potential game changer" in a June 2020 report. In January 2021, the global insurance brokerage Marsh named the Collective Defense platform as one of its industry-recognized Cyber Catalyst solutions. In August 2020, IronNet announced that it had achieved "FedRAMP-ready" for Agency Authorization status, as approved by the Federal Risk and Authorization Management Program (FedRAMP).

Table of Contents

Industry Background

Cybersecurity trends

There are a number of key trends driving the need for a new approach to cybersecurity.

Increased velocity of sophisticated attacks

Increasingly, adversaries are well-trained, possess significant technological and human resources, and are highly deliberate and targeted in their attacks. Adversaries today range from militaries and intelligence services of well-funded nation-states, to sophisticated criminal organizations motivated by financial gains, to hackers leveraging readily available advanced techniques. The broad availability and rapid evolution of cyber attack toolkits and use of regional cloud infrastructure or compromised servers to launch attacks make it nearly impossible for security teams to keep up with cyber threats. Given sufficient amount of time and resources, a determined adversary will have the ability to breach current cyber defenses of almost any enterprise, organization, or government.

Rear-facing and insufficient tools

Gartner, an industry research firm, estimates that worldwide spending on global information security will be \$186.2 billion by 2024, up from \$124.2 billion in 2018. Even with increased cybersecurity spending, however, security outcomes have not substantially improved. The recent widespread SolarWinds/SUNBURST cyberattack is just one example of how a sophisticated adversary can thoroughly permeate an industry, geography or supply chain. The lack of equally sophisticated threat intelligence sharing allowed this hack to penetrate networks more deeply, and for much longer. The evolving threat landscape has rendered traditional defense approaches incapable of protecting organizations against next-generation threats.

The current generation of security products focuses on signature-based approaches that often have limited ability to collect, process, and analyze vast amounts of data—attributes that are required to be effective in today’s increasingly dynamic threat landscape. This includes traditional and next-generation firewalls, Intrusion Detection and Prevention Systems (“IDPS”), SIEMs, and other similar tools that are designed to manage policies for network traffic and rely on rear-facing threat intelligence indicators of compromise (“IoCs”) based on IP, domains, file hashes and other signature-based intelligence from known threats. They are not fundamentally designed to detect advanced, never-before-seen, “unknown unknown” cyber threats in a timely and scalable fashion.

The borderless enterprise where the network is no longer the perimeter

Cloud, IoT and SaaS applications have expanded the attack surface and cyber vulnerabilities. According to a Gartner press release dated May 13, 2020, Gartner reports that, while some cloud transformation projects may have put on hold during the COVID-19 pandemic, it expects overall cloud spending levels previously estimated for 2023 and 2024 to show up as early as 2022. The ongoing COVID-19 pandemic has only accelerated this trend, with one survey by PricewaterhouseCoopers LLP reporting that 83% of executives believed the shift to remote work had been successful and that 79% of executives would no longer require a traditional five-day onsite work week. Furthermore, IDC, an industry research firm, estimates that by 2025 there will be 55.7 billion connected devices worldwide. The reality of the borderless enterprise will fundamentally change network cyber defenses from a centralized command and control defensive strategy using traditional on-premise blocking infrastructure to a distributed detect and respond strategy that fuses different sources of telemetry data across network, endpoints, and logs into actionable intelligence using large-scale behavioral analysis for security teams to take action.

Table of Contents*Scarcity of qualified human capital*

Even with the most sophisticated AI-based cyber technology in place, the human element of cybersecurity investigation, triage, and research plays an important role in risk reduction. As the Collective Defense platform is detecting and prioritizing anomalies, the analysts and threat hunters are ultimately deciding which alerts to triage, investigate, and manage through to response and mitigation. Organizations are consistently under-resourced in this area, however, as the ratio of the volume of network traffic versus the number of cybersecurity specialists to analyze that traffic is severely lopsided, resulting in Security Operations Center (SOC) staff overwhelm and burnout. A July 2020 report by the Information Systems Security Association states that 70 percent of its members believe that their organization has been impacted by the global cybersecurity skills shortage. The number of unfilled cybersecurity positions has already surpassed four million worldwide.

Cloud impact on enterprise cyber defenses

As digital transformation has accelerated in all industries, traditional security controls implemented on the company's on-premise network are often no longer available and often must operate differently for the outsourcing of IT infrastructure and operations to the public cloud provider. While the cloud is designed to make business easier, Management and Security Operations are different from traditional on-premise security, as the teams do not have access to the underlying networks or logs, and therefore have limited visibility of cloud infrastructure. The major cloud providers have introduced logging and basic detection using signature-based detection strategies, but these require additional third-party or custom capabilities to provide sufficient defenses. Security vendors have attempted to fill the security gaps by introducing new products for the cloud based on existing on-premise technologies, but these are often cloud bolt-ons that provide limited detection and visibility for cloud environments and are complex to deploy, difficult to scale, brittle to maintain, and costly to own.

Limitations of existing products

Existing detection and threat sharing methods have a number of limitations, including:

Legacy signature-based products

Signature-based products are designed to detect known attacks using a repository of previously identified indicators of compromise, but are not capable of detecting or responding to unknown threats. Used by network security, endpoint security, SIEMs and other standard defense-in-depth cybersecurity solutions as a core detection method, these signature-based detections have resulted in many significant breaches due to the failure of legacy defenses to detect a previously unknown or modified version of a previously known attack. While current technologies remain an essential part of the SOC Visibility Triad, a network-centric approach to threat detection and response described by Gartner in 2019, they miss a large swath of dangerous threats that evade detection, as evidenced by the major SolarWinds/SUNBURST supply chain and Microsoft Exchange server attacks widely reported in the news media in 2020 and 2021.

Log and event management products

SIEMs and similar log management products are designed for compliance, reporting, and security incident management purposes, but they struggle with the scale and processing required to deliver the behavioral-analysis capabilities across current and historical data to detect new or modified versions of known threats. While these systems provide useful correlation capabilities, security operation teams are increasingly leveraging these systems for central aggregation points for workflow, ticketing, and case management, rather than for detection.

[Table of Contents](#)*First generation network-based behavioral analysis products*

First generation network-based behavioral analysis products provide a basic level of outlier detection using Bayesian analysis or other statistical methods to identify obvious patterns in small networks. Often marketed as artificial intelligence (“AI”) solutions, these solutions lack the scale, correlation, or analysis capabilities needed to detect threats hiding in plain sight within networks commonly seen at mid-sized or larger enterprises with thousands of devices, hundreds of applications, multiple physical sites, and multi-cloud architectures.

Infrastructure monitoring/network performance monitoring and diagnostic-based products

Traditional network infrastructure providers offer infrastructure monitoring products designed to identify network bottlenecks and other network reliability or performance issues. Increasingly, these vendors have added bolt-on cybersecurity capabilities that can provide security teams’ networks with asset discovery and some network visibility, but they struggle with the algorithmic analysis needed to detect new and unknown threats with high fidelity or the forensic capabilities required by security operations team to investigate, triage, and respond to an identified network anomaly.

Threat intelligence sharing products

Threat intelligence products are designed to share massive amounts of non-specific signature-based IoCs that commonly focus on IP addresses and domains of known threats and often only after a substantial period of time by the contributing organization. The lack of timeliness or specificity to an enterprise severely limits the effectiveness of the shared information from a cyber defense perspective. By the time this information is shared, usually weeks or months after an attack, a sophisticated attacker only needs to slightly modify their methods by changing their attack infrastructure to enable them to bypass cyber defenses of their targeted enterprises, industries, or nations.

Information Sharing and Analysis Centers (“ISACs”) and other threat sharing groups

Threat sharing groups emerged more than 20 years ago as a way for security teams to work together to collect, analyze, and share actionable threat information within their members communities. IronNet believes this is a substantial step in the right direction; however, threat sharing in these groups relies largely on signature-centric threat intelligence platforms that struggle with timeliness and specificity of their intelligence or ad hoc manual forms of communication, such as email and only with a subset of security defenders with whom an analyst has a personal relationship. ISACs and similar groups are the right organizations, but they need technological solutions that enable them to share contextual, relevant, and timely information in real time across the full community.

Creating a new market segment: Collective Defense

“The U.S. government and industry ... must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This ‘collective defense’ in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense.”

— U. S. Cyberspace Solarium Commission Report, March 2020

IronNet is creating a new market category with Collective Defense. With its Collective Defense platform, IronNet developed the first and, to its knowledge, the only solution that can identify and rate anomalous behaviors on the network and share this anonymized threat intelligence among Collective Defense community members (who may comprise a supply chain, state, or country) as an early-warning system for all.

Table of Contents

The power of Collective Defense is that multiple companies can essentially work as a team to detect and defend against attackers early in the network threat intrusion cycle. This differentiated approach allows customers to:

Gain real-time visibility across the threat landscape

IronNet's Collective Defense platform leverages proven behavioral analytics, machine learning ("ML"), and AI techniques across anonymized participant data to identify stealthy, sophisticated threats that otherwise may be missed by an individual enterprise and signature-based tools. The platform has been designed to deliver real-time visibility of cyber threats targeting supply chains, industries, regions, or any custom IronDome Collective Defense grouping.

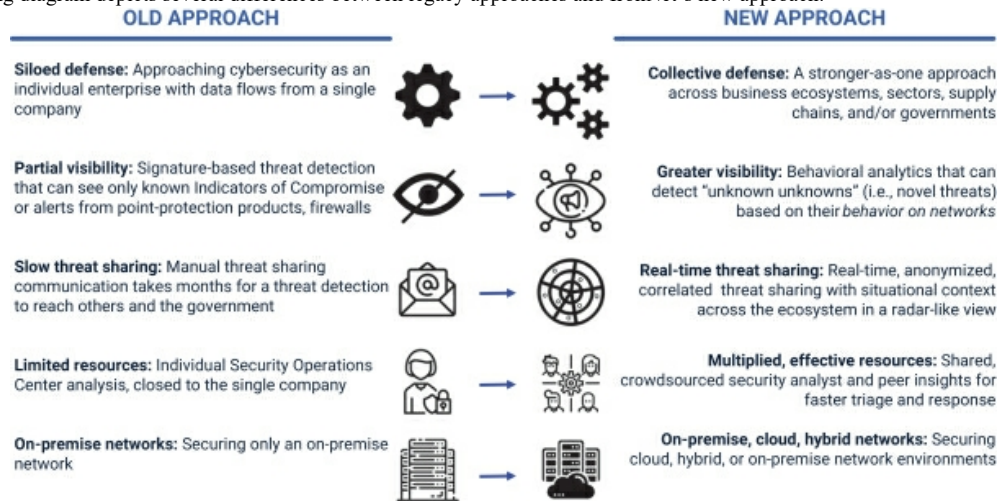
Reduce impact of cyber attacks with help from fellow cyber defenders

The Collective Defense ecosystem acts as a collaboration hub to enable participants to automatically share real-time detections, triage outcomes, threat indicators, and other insights with members of their Collective Defense group. When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members at machine speed so each member can prioritize their defense against the identified cyber threat.

Improve effectiveness of existing cybersecurity investments

Threat intelligence is valuable, actionable, and relevant only when received in time, before a threat enters a network. IronNet's innovative collective threat intelligence provides immediate alerts at machine speed and context into urgent threats, enabling organizations to prioritize threats and build a proactive defense. This information can be used by a customer's existing network, endpoint, or other security tools to identify and stop adversaries from retargeting their attack.

The following diagram depicts several differences between legacy approaches and IronNet's new approach:



A new cybersecurity model: from reactive, individual defense to proactive, Collective Defense

[Table of Contents](#)**IronNet's Solution: The Collective Defense Platform**

The Collective Defense platform comprises two tightly integrated proprietary technologies: IronNet's Network Detection and Response (NDR) solution, IronDefense, and its innovative collective threat-sharing solution, IronDome.

The IronNet Collective Defense platform offers a unified set of technologies that powers a wide range of network behavioral detection, security operations, real-time threat landscape visibility, threat sharing, and peer SOC-analyst collaboration capabilities. IronNet can rapidly and cost effectively deploy in its customer's public cloud, private cloud, and on-premise infrastructure using its flexible deployment options. Its expanding set of open APIs and ecosystem integrations enable it to add new sources of data for behavioral analysis and Collective Defense sharing and collaboration to detect and stop targeted cyber attacks.

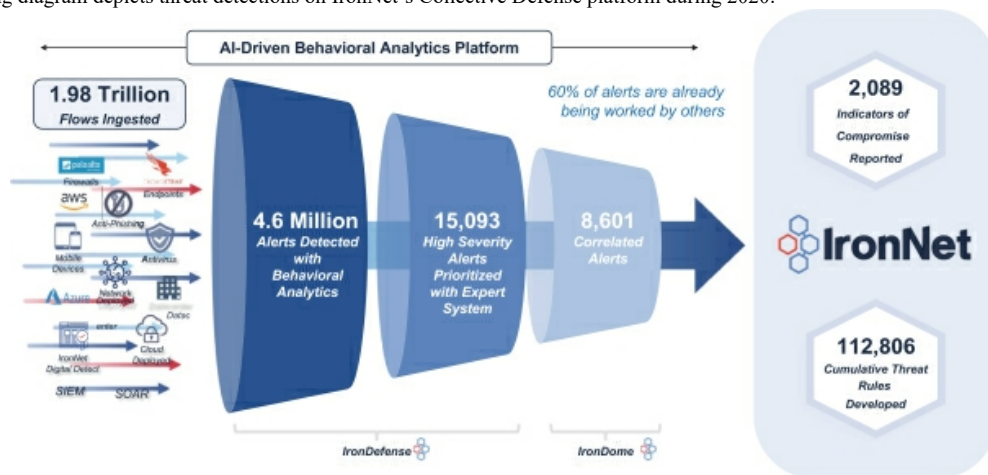
Armed with elite detection capabilities and combined offensive operator experience at the highest level of the U.S. government, IronNet's founders set out to build a behavioral analytics solution to detect threats heading toward, or already in, the network. A growing portfolio of proprietary analytics forms the backbone of IronDefense. However, while effective in detecting unknown anomalies, behavioral analytics by itself is insufficient in modern, noisy networks where anomalies are common and can lead to a high number of false positives. For many NDR vendors in the industry, the solution is to tune their analytics to be less sensitive in order to deliver reduced false-positive rates at the expense of letting true positives into the network. IronNet undertook a different strategy to meet this challenge. It introduced its expert system scoring algorithms, supported by IronNet's elite cyber hunters, to increase its detection specificity while preserving the sensitivity of its analytics in IronDefense.

IronNet introduced IronDome in 2018. Powered by IronDefense's threat detections, IronDome is the foundation of IronNet's Collective Defense platform, a purpose-built, cloud-native, and holistic platform that is capable of defending, analyzing, and correlating threats from various sources. It delivers timely, actionable, and contextual insights to attacks targeting an enterprise and, from there, is able to provide early warning to all members of the Collective Defense ecosystem.

The differentiated value of IronNet's Collective Defense platform is its ability to build a dynamic, comprehensive picture of the threat environment, much like radar for cyberspace, based on real-time, anonymized alert correlation across any participating member environments. It also provides situational context and peer insights for greater visibility and context of the threat landscape at any given time.

Table of Contents

The following diagram depicts threat detections on IronNet's Collective Defense platform during 2020:



Notes: Represents full-year data for calendar year 2020 except for cumulative number.

Correlated alerts for threat detection earlier in the intrusion cycle

IronNet is not aware of any other vendor in the market with a similar approach to cybersecurity. Even though community members bring disparate network environments, such as cloud, on-premise or hybrid, to the Collective Defense ecosystem, correlated threats stand out given that the adversarial behaviors are typically consistent, no matter who the target is, as was the case with the SolarWinds/SUNBURST attack.

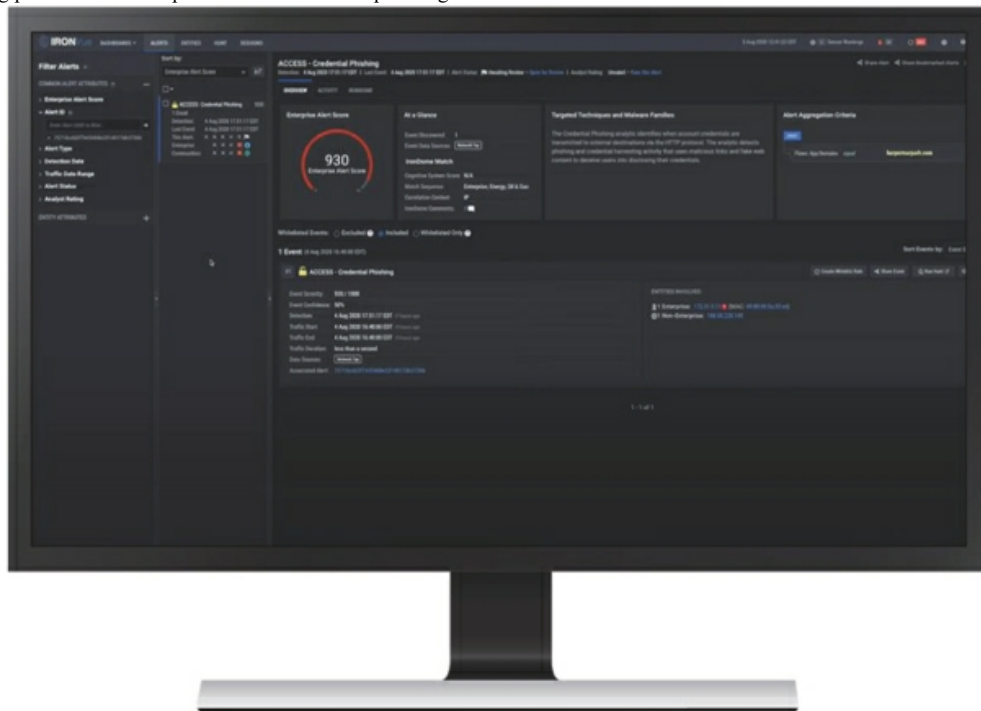
The Collective Defense platform comprises two flagship products:

IronDefense

IronDefense is an advanced Network Detection and Response (NDR) solution that provides behavior-based and AI-driven analytics at the network level to detect anomalous activity at individual enterprises and prioritize the highest threats in a company's network. IronNet leverages novel AI/ML algorithms to deliver high-fidelity analytics required to detect previously unknown threats. In addition, IronNet provides advanced enrichment techniques via IronDefense's Expert System, which has been designed to achieve high efficacy levels, low false positive rates, and improved visibility compared to legacy approaches. This is all done at network speed and cloud scale.

Table of Contents

The following picture shows a representative credential phishing detection in IronDefense.



Most current cybersecurity tools focus on detecting the final “action-on-target” step of an intrusion. At this stage, identification is easier but the insights come far too late to stop attackers from getting into positions in the network to exfiltrate data, steal IP, or accomplish other malicious objectives. IronDefense uses advanced analytics based on metadata from the traffic in the customer’s network to identify anomalous activity earlier in the intrusion kill chain.

Key components of IronDefense include:

IronDefense behavioral analysis engine

IronDefense leverages behavioral-based detections to identify threats targeting industries and companies earlier in the intrusion cycle, and to identify the underlying behavior and methods to counter unknown threats, or customizations that attackers will implement to target companies in the future. The analytics are built upon algorithms that form the foundation of the patented IronDefense platform. They are computationally designed to understand normal network behavior by applying tests to create a benchmark of standard, acceptable traffic patterns in the network. Detected anomalies are grouped with similar instances of traffic behavior to minimize alerting and to aggregate events by events within the customers’ networks.

IronDefense Expert System

IronDefense includes an Expert System that automates security operations playbooks of how top cyber operations hunters leverage contextual data and other sources of telemetry data later on in the detection and

[Table of Contents](#)

response process and applies it to the risk scoring of anomalies detected by its behavioral analysis. This enables IronNet to preserve its detection accuracy without sacrificing the sensitivity of its algorithms by leveraging the wisdom of IronNet's elite cyber hunters triaging thousands of alerts from real-world environments. The expert system also alleviates the "alert fatigue" that plagues every SOC by minimizing the tedious steps in an investigation, reducing alert fatigue and allowing security teams to focus on responding to high risk detection in their environments. The Expert System is continually optimized through machine learning from anonymized triaged outcomes by IronNet cyber hunters using IronDefense.

IronDefense CoDA engine

Threat analysts and hunters spend a significant portion of their time triaging individual alerts by identifying corroborating evidence and related information. In 2021, IronNet is launching a new correlation engine called CoDA, for Correlation of Detections and Alerts, that models adversary attack techniques and pre-correlates anomalous activity by threat categories to improve risk scoring and alert prioritization, as well as to dramatically reduce alert load. This system leverages a multi-pass system that first optimizes for detecting as many potential instances of a particular type of threat activity and enriching detections with threat intelligence and other external and internal data sources to optimize for detection precision. Events are further aggregated by entity information, attack stage identification, and time sequence data to deliver a timeline of an attack and scored by risk to the enterprise.

IronDefense threat hunting interface

IronDefense includes a threat hunting interface built by IronNet's elite cyber hunters to empower security operations teams to conduct detailed investigative workflows and forensic analysis of threats detected by IronDefense. The hunting interface empowers security analysts to investigate across all raw traffic, network metadata, logs, telemetry data, and collective threat intelligence captured by IronDefense, all the way down to full-packet capture of individual network flows.

IronDefense sensors

IronDefense sensors are cloud, virtual, and physical sensors that are deployed at the network perimeter to ingest "north-south" traffic within internal networks to provide "east-west" traffic visibility across an enterprise. Cloud sensors are available for public cloud environments to ingest raw traffic data directly from Infrastructure-as-a-Service ("IaaS") virtual networks from major cloud providers such as AWS and Microsoft Azure deployments. The sensor extracts rich network session metadata from the raw traffic and sends it to IronNet's behavior analysis engine for processing and expert system validation. The IronDefense sensors also continuously collect full raw traffic packet capture for inspection during hunting operations.

IronDefense direct data ingest

IronDefense has the ability to utilize a wide-range of data types and telemetry data directly from existing sources. These data sources include standard protocols such as DNS, HTTP/S, or Active Directory; common network log formats such as BRO/ZEK or NetFlow; Cloud Provider logs such as AWS VPC, AWS CloudTrail or Microsoft Azure NSG logs; and application logs such as Office 365.

IronDome

IronDome is a threat-sharing solution that facilitates a crowdsourced-like environment in which the IronDefense findings from an individual company are automatically and anonymously shared within groups of related entities, such as portfolio companies, supply chains, industries, or nations, for correlation and further analysis. IronDome analyzes threat detections across companies to identify broad attack patterns and provides anonymized intelligence back to all customers in real time.

Table of Contents

IronDome enables Collective Defense member enterprises to actively share individual anonymized cyber anomalies at machine speed across a community of public-private peers. This capability allows companies to identify stealthy attackers earlier in the attack cycle when many of their methods fall below the threshold of detection at a single company by allowing companies to aggregate data and run higher-order analysis across industry data.

Key components of IronDome include:

IronDome Collective Defense communities

IronDome threat sharing is organized by communities of enterprises based on their business ecosystem, industry, region, or nation. Enterprises can be members of multiple communities based on their sharing preference and threat sharing needs. As customer adoption grows, the network effect of each additional enterprise participating in IronNet's Collective Defense platform will amplify the breadth and depth of its dataset and intelligence.

IronDome collective threat intelligence sharing

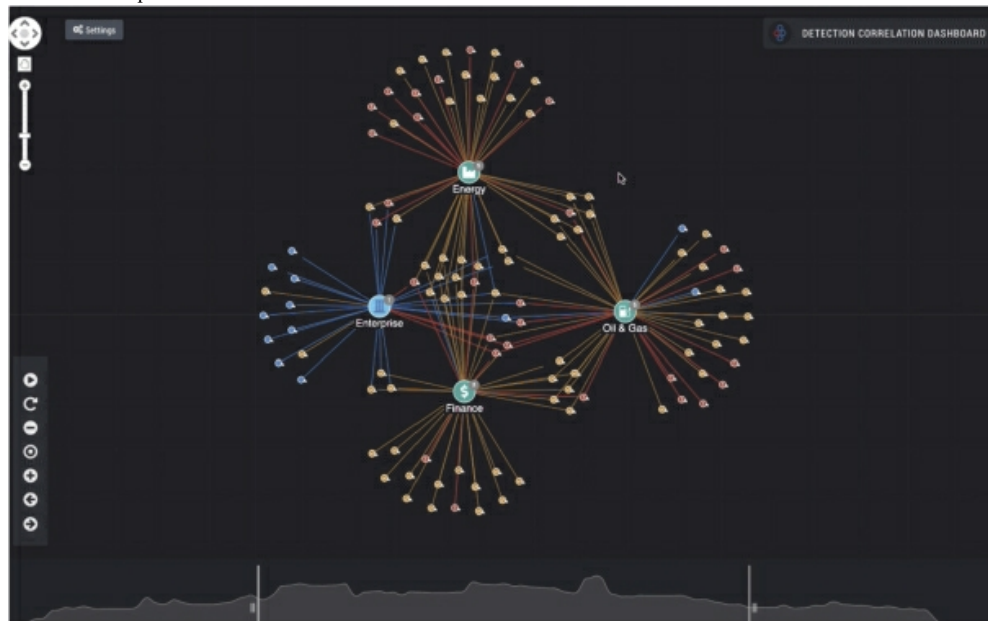
IronDome links communities of enterprises together to provide contextual insights into the threat landscape. Machine and human intelligence is shared in real time across the community by threat correlations, as well as outcomes and insights related to how various analysts at different enterprises rated and triaged similar threats in their environment. Real-time feedback of these insights delivers enhanced threat landscape visibility and detection insights that allow members to immediately react to active threats targeting their industry and to adjust their defenses to combat the threat.

IronDome RadarView

IronDome creates a radar-like view of cyberspace that links private and public sector stakeholders in their Collective Defense community. The RadarView graph provides an anonymized real-time view of threats targeting an enterprise's business ecosystem, supply chain, industry, or region.

[Table of Contents](#)

The following picture shows a sample Detection Correlation Dashboard in IronDome.



Called Collective Defense communities, spearheaded by a “cornerstone” company or organization, an IronDome could be established for a company’s business ecosystem, such as a wealth management firm with many portfolio companies; a sector-based collaborative, such as in within energy or finance), or a cross-sector formation; states and countries; and private-public sector configurations.

In each Collective Defense community, members agree to share anonymized data about threats detected on their individual networks with the collective, on an ongoing basis. This collaborative approach is designed to “flip the script” on attackers by raising the defensive capabilities of any one player. If correlated alerts and attribution based on behaviors suggest that a nation-state is involved, Collective Defense participants can voluntarily share threat information with the government for cyber defense on a national scale as needed to defend the nation.

The Collective Defense platform is available for on-premise, cloud (public and private), and hybrid environments, and it is scalable to include small-medium businesses as well as multinational corporations.

Threat Intelligence

Using information derived from the Collective Defense Platform, IronNet also provides its customers with threat intelligence.

IronNet Threat Intelligence Rules

IronNet develops threat intelligence rules (“TIRs”) based on significant community findings. These detection rules for network, endpoint, or other security tools allow customers to proactively protect themselves against known threats through more secure controls.

[Table of Contents](#)*IronNet Threat Intelligence Brief*

The monthly IronNet Threat Intelligence Brief provides top observed threats across IronNet Collective Defense communities. It includes significant community findings, such as network behavioral anomalies that were rated as suspicious or malicious by IronNet and/or participant analysts, threat intelligence rules, a snapshot of monthly correlated alerts, and threat research highlights.

Key Benefits of IronNet's Solution

IronNet's solution offers its customers several benefits, including:

- differentiated business value that includes behavioral analytics, which find threats that other tools cannot;
- real-time threat-sharing across communities; and
- value to the Collective Defense ecosystem through integrations.

These benefits are summarized in the graphic below.

***Behavioral analytics that find threats that other tools cannot detect****Superior threat behavior detection to see unknown threats*

IronDefense examines the network traffic itself, which is much harder for an attacker to evade or manipulate. IronDefense threat detections are based on advanced, high-fidelity analytics and AI/ML detection capabilities built by top cyber subject matter experts (“SMEs”), continuous full packet capture (“PCAP”), an expert system that applies the judgment and tradecraft playbooks of the nation’s top cyber defenders, and integrated cyber hunting (packet level visibility that improves speed and depth of investigations).

Visibility across the full enterprise to close threat detection gaps

IronDefense network detections fill the known void in threat visibility, which is being able to see unknown, novel threats on the network that other tools cannot see. The Collective Defense platform is an essential part of the SOC Visibility Triad, complementing endpoint detection and response (EDR) and logs. It is the engine that can transform this triad into a dynamic pyramid for comprehensive visibility across the threat landscape.

Table of Contents*Cognitive detection, correlation, and prioritization analytics for reduced false positives*

The Collective Defense platform collects, processes, correlates, and analyzes high-fidelity data from customer networks (anonymized), threat intelligence on real-world attacks, significant community findings, and correlated alerts in the Collective Defense communities. IronNet uses this data to continually train and enhance its IronDefense behavioral analytics to increase the signal-to-noise ratio to detect new, unknown attacks with high-fidelity analytics. IronNet automatically chains and scores related events into signals to increase analyst visibility.

Data ingest at scale for a broader view of the threat landscape

IronDefense gathers data streams from a variety of sources to build a more comprehensive picture of threats. Network sensors provide streaming capture of all network packets for detection and visibility into all protocols activity. Network logs provide asset discovery and device metadata for event enrichment and contextualization. Cloud data on user activity and usage patterns only the cloud provider can collect. Security ecosystem data provide entity and user operational state which supplements network and cloud data collected.

*The only real-time threat sharing capability across companies for stronger defense**The ability to defend better as a collective force*

The Collective Defense platform orchestrates threat-sharing and collaboration in real time to deliver immediate visibility and instant sharing of malicious cyber threats targeting supply chains, industries, regions, or any custom Collective Defense community to reduce impact of cyber attacks with help from fellow cyber defenders. IronDome acts as a collaboration hub to enable members to automatically share real-time detections, triage outcomes, threat indicators, and other insights with members of their Collective Defense community.

Faster warning and response capabilities

When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members at machine speed so each member can prioritize their defense against the identified cyber threat. This capability allows companies to identify stealthy attackers earlier in the attack cycle when many of their methods fall below the threshold of detection at a single company by allowing companies to aggregate data and run higher-order analyses across industry data. The platform supports opt-in anonymized sharing with governments for national response when necessary.

Real-time sharing of peer insights for stronger defense

The Collective Defense platform allows community members to share threat context, prevalence, and expert commentary about how to triage and response, much like the Waze app for traffic, except for cybersecurity. By banding together and working together with peers, Collective Defense community members are better able to pool and optimize resources so they can achieve “defensive economies of scale” that allow them to keep up with and counteract cyber attackers.

Deep subject matter expertise to improve customer defense

IronNet has an elite cyber operations team working directly with customers’ security teams to detect, triage, and respond. Its teams are led by cyber offensive and defensive SMEs. Approximately one-half of IronNet’s cyber operations experts have National Security Agency or U.S. Department of Defense experience, and 40% have cyber offensive, intel, or research experience.

A force multiplier effect to help strained SOC teams

IronNet’s deep SME knowledge enables a multiplier effect for severely strained SOC analysts, who can leverage insights from its security analysts and threat hunters, as well as peer insights and triage outcomes from

Table of Contents

the Collective Defense community. This approach addresses the cyber talent shortage, improving the effectiveness of SOC teams and optimizing tools and human resources. IronNet's high-fidelity analytics and threat intelligence provide autonomous identification, prioritization, and recommendation to accelerate incident investigation and the response process.

Added value to the cybersecurity ecosystem***Easy-to-use deployment for faster time to value***

The Collective Defense platform has been designed to be easy to provision, configure, and manage, working seamlessly with a suite of SIEM, SOAR, EDR, and NGFW APIs to streamline siloed security products. These integrations provide a natural complement to IronDefense and reinforce the users' existing security infrastructures. Analysts do not need to re-learn anything and can see detections from a single view.

Security for any environment

IronNet can provide security protection across cloud, multi-cloud, on-premise, and virtual environments to support customers with different needs. Public cloud options are Amazon Web Services ("AWS") and Microsoft Azure, and IronNet has private cloud options based on Nutanix for customers that want to leverage their own on-premise HCI environments. The on-premise deployment option is IronNet's hardware appliance or virtual application.

Improved effectiveness of existing security investments

IronDefense automates many of the time-consuming threat discovery and investigation steps and indicates the severity of anomalous activity. Its customers' analysts can make decisions in a shorter amount of time.

Industry Recognition, Awards and Designations***Industry analyst reports***

Over the past 24 months, IronNet and its platform and products have been recognized in 10 reports by multiple third-party industry analysts, including Gartner, Forrester, IDC, 451 Research Group, and Omdia, who has called IronNet's analytics a "potential game changer" in a June 2020 report.

Industry designations***Cyber Catalyst by Marsh™ designation***

In January 2021, the global insurance brokerage Marsh named the Collective Defense platform as one of its industry-recognized Cyber Catalyst solutions. This evaluation program is designed to help organizations make more informed choices about cybersecurity products and services to manage their cyber risk, by providing independent reviews conducted by insurers who fully understand the impact of risk exposure.

FedRAMP Ready for Agency Authorization

In August 2020, IronNet announced that it had achieved "FedRAMP ready" status for Agency Authorization status, as approved by the FedRAMP. IronNet's achievement of this status means the FedRAMP PMO has determined that IronNet can meet the FedRAMP security requirements and could be granted an Authority to Operate ("ATO") from federal agencies.

Industry certifications***GDPR-compliant***

IronNet is committed to data privacy and is compliant under the European Union ("EU") General Data Protection Regulation ("GDPR"). IronNet is also an active member of the EU/ Swiss-US Privacy Shield

Table of Contents

Framework through the U.S. Department of Commerce. The EU/Swiss-U.S. Privacy Shield Framework provides a method for companies to transfer personal data to the United States from the EU in a way that is consistent with EU law and acceptable under EU GDPR.

ISO/IEC 27001

ISO 27001 is an international standard for information security management systems (“ISMS”). An ISO 27001 certification demonstrates that IronNet has addressed the following areas: security policy, organization and information security, asset management, human resources security, physical and environmental security, communication and operations management, access control, information systems acquisition, security incident management, business continuity management, and compliance.

SOC2 Type I and SOC2 Type II

IronNet is also SOC2/Type I and Type II certified, verifying that it has a suitable design of controls to meet the criteria for the security, availability, confidentiality, and processing integrity principles of the SOC2 standard. Having Type II attestation demonstrates the operational effectiveness of IronNet’s design controls.

Department of Homeland Security Continuous Diagnostics & Monitoring

IronNet is registered with The Department of Homeland Security (“DHS”) Continuous Diagnostics & Monitoring (“CDM”) program recognizing cybersecurity tools and sensors that are reviewed by the DHS program for conformance with Section 508, federal license users and CDM technical requirements. IronNet also received two separate acceptances/approvals for the DHS CDM Approved Products List for IronDefense (IRO-0002-20180103) and IronDome (IRO-0004-20180405).

Industry Award highlights***2020 Fortress Cyber Security Award***

IronNet won a Fortress Cyber Security Award for two years in a row in the Public & Private Cloud category for IronDome. The award recognizes the world’s leading companies and products that are working to keep data and digital assets safe.

2020 CyberSecurity Breakthrough Award

IronNet’s IronDome Collective Defense solution was named the “Overall Incident Response Solution of the Year” by the 2020 CyberSecurity Breakthrough Awards. The CyberSecurity Breakthrough Awards program recognizes the top companies, technologies, and products in the global information security market.

2020 Cyber Security Awards

IronNet’s IronDome Collective Defense platform was named the winner of the “Innovative Product of the Year—Threat Detection” by the Cyber Security Awards. The Cyber Security Awards recognize the best individuals, teams, and companies within the cybersecurity industry for excellence and innovation across 18 categories.

2020 CRN Emerging Vendors List

IronNet was named to the 2020 Emerging Vendors list in the Security Channel by CRN. This annual list honors new, rising technology suppliers that exhibit great promise in shaping the future success of the channel with their dedication to innovation.

[Table of Contents](#)

IronNet's Market Opportunity

"Information sharing is critical for empowering the global ecosystem to move from individual to collective cyber resilience."

— World Economic Forum Centre for Cybersecurity,
"Cyber Information Sharing: Building Collective Security," October 2020

IronNet was founded on the belief that network defense accelerated by AI was the future of cybersecurity and that the ability to share these AI-based threat detections in real time was non-existent in the market at the time of IronNet's inception. IronNet's goal has been to give companies, organizations, and governments better ways to fight back against organized criminal groups and nation-state adversaries.

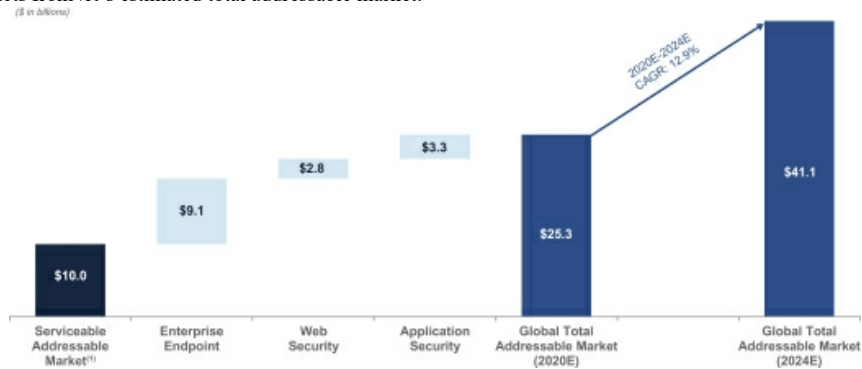
To best operationalize AI in a security setting, IronNet turned to the ML subset of AI. It uses ML models to detect "unknown unknown" threats to networks. An unknown threat, or a zero-day threat, is considered a malicious code that has not been seen before, hence without a "signature." Such threats exploit vulnerabilities as advanced persistent threats or targeted attacks. Behavioral analytics, which are data-driven algorithms tuned to detect behaviors on networks, can increase an organization's visibility across the network, reduce the impact of cyber attacks, and improve the effectiveness of their cybersecurity investments.

IronNet believes there is a clear market need to systemically fix a broken approach to cybersecurity. According to the Center for Strategic and International Studies, global cybercrime losses have nearly doubled from \$523 billion in 2018 to \$945 billion in 2020. Being able to detect unknown, malicious threats and share threat intelligence through Collective Defense is critical for mitigating the impact on business continuity and cost. An independent industry study conducted in 2020 estimates that it takes an average of 315 days to detect and contain a data breach caused by a malicious attack, while an average of 230 days is necessary to identify a malicious breach, giving hackers dangerous network dwell time to steal personally identifiable information (at the average cost of \$175 per record in malicious attacks) and intellectual property. Security automation can reduce that lifecycle by about 2.5 months. Shortening the detect-to-contain cycle to less than 200 days could potentially cut the total cost by about a quarter.

[Table of Contents](#)

Market Overview

The following graphic depicts IronNet's estimated total addressable market:



Source:Gartner: Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 4Q20 Update

- (1) Summation of revenues generated from solutions for Security Information and Event Management (SIEM) Software, IDPS Equipment, Enterprise Data Loss Prevention, Threat Intelligence Software, Network Detection and Response, and Network Access Control.

IronNet's customers utilize its Collective Defense platform across a wide variety of use cases. Its total addressable market initially began as a behavioral-based detection and response opportunity in the network security market, but has significantly expanded due to rapid innovation and adoption of the Collective Defense platform across additional security segments.

In addition, IronNet's increasing market opportunity is driven by the rapidly increasing desire and willingness of public and private enterprises of all sizes to share collective threat intelligence and work together in common defense to support their continued acceleration of digital transformation and cloud computing, adoption of the Internet of Things ("IoT"), and the ability to defend their enterprises in a continually intensifying threat landscape.

IronNet's innovative approach is unique in the security industry. IronNet identifies anomalies across network traffic using advanced behavioral analytics, artificial intelligence, and machine learning techniques; applies integrated security operations automation through the use of its Expert System; automatically correlates pre-triaged detections; and shares collective threat intelligence across an enterprise's business ecosystem. Because of its solution strategy and architecture, the IronNet Collective Defense platform is the first to address multiple security markets, including markets not typically associated with Network Detection and Response.

The markets IronNet addresses comprise the following:

Network Security Equipment and Infrastructure Protection

In 2016, IronNet launched its IronDefense product to disrupt the Enterprise Network Security Equipment market that included what is now the NDR, Network Access Control ("NAC"), and Intrusion Detection & Prevention System ("IDPS") markets, respectively. As part of its launch of IronDefense, it included a security operations capability built by world-class security experts specific for security operations to address the SIEM and Enterprise Data Loss Prevention ("DLP") markets, respectively. In 2018, IronNet launched its IronDome product to disrupt the threat intelligence market by providing enterprises with real-time visibility to their threat landscape and curated threat intelligence to actual threats targeting their business ecosystem, supply chain, industry, and region. Gartner estimates that the global market for these segments in the Network Security Equipment and the Infrastructure Protection will be \$10.0 billion in 2021.

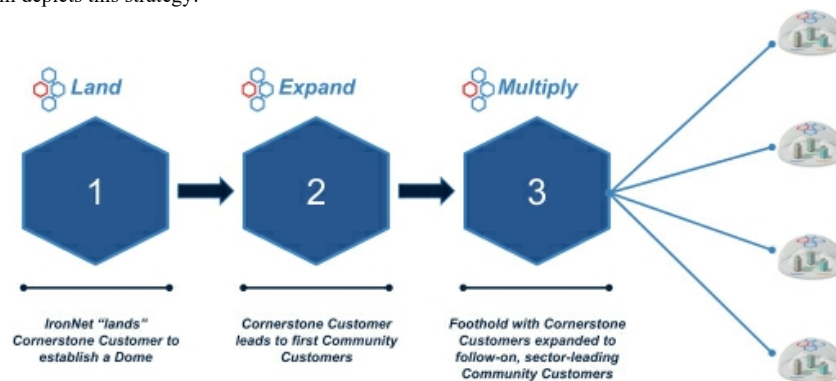
[Table of Contents](#)*Application Security, Web Security, and Enterprise Endpoint*

Additional enhancements in 2020 to IronDefense and IronDome that further enable use to operate in public cloud environments allow IronNet to address the Application Security segment and web security market that Gartner estimated at \$3.3 billion and \$2.8 billion, respectively, in 2020. The addition of ecosystem integrations in 2021 across a range of security ecosystems increases IronNet's footprint within a security ecosystem, and its ability to work natively with endpoint detection and response vendors under its Collective Defense capabilities enables IronNet to address the enterprise endpoint market, which Gartner estimated at \$9.1 billion in 2020.

IronNet's Go-to-Market Strategy

IronNet describes its go-to-market strategy as "land and expand with network effects." Its approach is to initially secure what it describes as influential "cornerstone" customers and then to expand their respective Collective Defense community with additional "community members" from organizations of similar industry sector, state, country, supply chain, or tailored business ecosystem. As each Collective Defense community grows, so does the volume of shared data, and the value of IronNet's platform for each of those members thereby expands both technically and commercially.

The following diagram depicts this strategy:



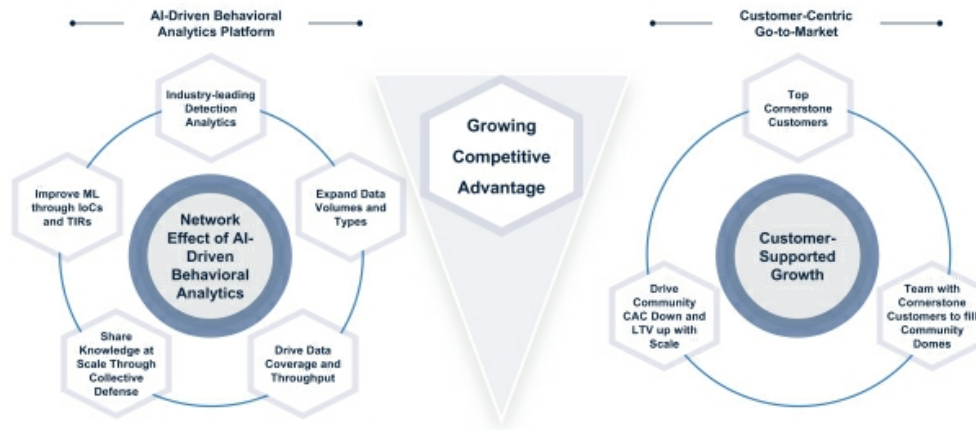
IronNet defines a Collective Defense cornerstone customer as a customer who is a leader of a recognized industry, nation, state, or vertical. Example of cornerstone customers include the U.S. government, with the defense industrial base, whereby a large systems integrator, along with a branch of the military, that are securing their thousands of supply chain members within a Collective Defense community. Another example is a global investment fund in the Asia Pacific Japan region with a \$300 billion portfolio. IronNet's relationship with this fund led to securing a single portfolio company as a community customer, and IronNet has now expanded to multiple companies within the fund's portfolio.

By securing business with organizations that are influential in their sector, proving its value through its Collective Defense solution, and partnering with their senior leadership, IronNet believes it can sell into similar organizations effectively and with great credibility.

IronNet's emphasis on information sharing has also helped it find particular success working with key industry associations, such as the Electricity Information Sharing and Analysis Center, or E-ISAC, to capitalize on the strong relationships and shared goals among member organizations. By becoming a trusted thought leader responding to their shared challenges in cybersecurity, IronNet seeks to gain access to potential customers while providing cybersecurity insight, instruction, and advice to the association as well—a core tenet of its Collective Defense mission.

[Table of Contents](#)

The overall effect of its go-to-market approach drives two powerful network effects, which are depicted in the graphic below. The first is the growth in the value of IronNet's platform as it ingests more and different data to improve the detection of its machine learning-driven algorithms. The second is its customer community-driven growth model, which drives a more efficient route to market with lower community customer acquisition costs and higher customer lifetime values.

***IronNet's Growth Strategy***

IronNet sees the opportunity for multi-dimensional innovation and growth. IronNet believes that the SolarWinds/SUNBURST attack in 2020 has validated its mission to drive AI-driven behavioral analytics and Collective Defense to the overall security market.

IronNet's revenues have grown steadily since its first product release in 2016. It made its first moves to the cloud in 2018, and it intends to accelerate scalability from its cloud offerings. This evolution in IronNet's products allow it to deploy to customers more rapidly, scale more quickly, and drive revenue growth.

IronNet's strategies to grow its business include the following:

Grow its customer base by replacing legacy and other NDR products

Given the limitations of existing products in the NDR, SIEM, IDPS, EDLP, and Threat Intelligence Software segments, IronNet intends continue to grow its customer base organically as organizations replace these signature-based and stand-alone offerings with AI-driven behavioral analytics and Collective Defense. Its customer acquisition campaigns and channel partnerships with MDR providers are expected to allow IronNet to pair pursuit of large enterprise customers with cost-effective penetration into smaller and medium-sized enterprises.

Further expand offerings with existing customers

IronNet will continue to expand its relationships with its customers by expanding its network coverage of their business towards 100% and by cross-selling additional Collective Defense offerings. When IronNet first deploys its products to a customer, it usually covers only a portion of their network traffic. As IronNet is able to demonstrate the value of its behavioral analytics and membership in Collective Defense, it has up-sell

[Table of Contents](#)

opportunities as it expands network coverage to other parts of the business or portfolio. IronNet also has the opportunity to cross-sell offerings like cloud traffic analytics or digital fraud detection. Over time, IronNet seeks to deploy its solutions enterprise-wide for all customers, thereby increasing its revenue from existing customers and therefore its dollar-based net retention rates.

Expand into new customer segments

While IronNet first targeted large and sophisticated enterprise customers, it also has an internal sales development team and an inside sales team to expand its go-to-market efforts. These teams focus on early qualification and development for cycles with potential cornerstone customers. They utilize intelligence from IronNet's Account Based Marketing system as well as social sales development tools to nurture these opportunities to a handoff point with field sales. These teams also focus on full cycles with potential community members once a cornerstone-driven Collective Defense community has been established. IronNet is using a combination selling approach to scale its sales into additional industry verticals, with which it can sell its Collective Defense capabilities to the largest enterprises or smallest businesses with any level of security sophistication and budget.

Extend its Collective Defense platform and ecosystem

IronNet designed its architecture to be open, interoperable, and highly extensible. It is constantly adding integrations to its platform in order to ingest more sources of data for analysis and to provide detection outputs to more response systems. IronNet also adds new algorithms and new combinations of algorithms to detect behaviors of unknown but potentially malicious attacks. In addition, IronNet innovates with partners to add IronNet NDR and Collective Defense capabilities to their customer offerings. An example of this is IronNet's recent announcement of a strategic partnership with Jacobs Engineering Group, an international technical professional services firm, under which the parties will work together to develop an end-to-end solution designed to detect and prevent damaging and difficult-to-detect cyberattacks that continue to plague organizations across public and private sectors. The joint offering of Jacobs' managed services capabilities and IronNet's advancements in machine learning and AI provides their respective customers a more thorough approach to network security. IronNet expects that innovations and partnerships such as its partnership with Jacobs will enhance the distribution of its platform and represent future sources of revenue.

Broaden reach into the U.S. federal government vertical

IronNet spent the first five years of its life building foundational customer relationships in the commercial sector. This was intentional, as its company mission required it first to build the technology and business basis required to protect the private side of the public/private partnership. IronNet is now actively investing in the acquisition of customers in the U.S. federal government vertical. IronNet is FedRAMP Ready and is registered with the Department of Homeland Security Continuous Diagnostics & Monitoring program approved products list to provide federal agencies with innovative security tools. In addition, its platform is deployed in the AWS GovCloud. IronNet is pursuing opportunities in the civilian, defense, and intelligence sectors.

Expand its international footprint

IronNet is expanding its international operations and will continue to invest globally to broaden its international footprint. IronNet intends to grow its presence in the Asia Pacific Japan and EMEA regions by adding headcount and establishing overseas hosting relationships.

[Table of Contents](#)**IronNet's Technology*****Cloud-native architecture***

IronNet's platform is designed to be secure, highly scalable, redundant, resilient, and high-performing. Delivering from the cloud is intended to enable agility, ease of use, and flexible detection of threats within individual enterprises and the correlation and sharing of those insights with their broader Collective Defense communities. Individual enterprises can choose to deploy IronNet using a variety of public and private cloud deployment options including AWS and Microsoft Azure. Enterprises that prefer to leverage their own private cloud infrastructure using hyper converged infrastructure can deploy IronNet through its partnership with Nutanix.

Flexible architecture for all enterprise networks

IronNet's Collective Defense platform enables enterprises to add behavioral detection and Collective Defense to their on-premise, cloud, or multi-cloud infrastructure. IronNet's platform can monitor workloads in major public cloud providers and on-premise physical and virtual networks from a single platform. IronNet's Collective Defense platform can monitor network traffic and raw traffic in AWS and Azure or leverage existing logs to detect threats targeting their cloud infrastructure. With IronNet, enterprises can apply the power of IronNet Collective Defense to their IT infrastructure and share collective threat intelligence with their Collective Defense community to detect threats targeting their community.

APIs / integrations

The Collective Defense platform and architecture is built around a rich set of APIs intended to efficiently and effectively complement and expand a customer's existing security infrastructure, such as SIEMs, EDRs, NGFWs, ITSM workflow tools, and other common cybersecurity tools. The platform includes the ability to query and interact with these tools, allowing customers and partners to integrate its detection into their security operations and to execute native response against detected threats. By connecting existing security systems to the IronNet Collective Defense platform, IronNet allows its customers to drive higher efficiencies and value from their security investments. For example, IronNet integrates with CrowdStrike to provide 1-click containment and can leverage CrowdStrike information to provide host details in the IronDefense Threat Hunting interface to deliver a seamless security operations experience across network and devices.

Data center operations

The Collective Defense platform utilizes a combination of global and customer infrastructure to deliver the solution. Customers can choose a variety of deployment options for their own enterprise however global and Collective Defense community level information is hosted in AWS data centers located in the United States and regional AWS data centers to support IronNet's international business. IronNet's technology infrastructure, combined with the use of AWS resources, provides it with a distributed and scalable architecture on a global scale.

IronNet's Services***Cyber Operations Center (CyOC)***

IronDefense customers can extend their SOC with IronNet's dedicated CyOC team, which comprises expert offensive and defensive cybersecurity operators with experience defending both private and public sectors against sophisticated threats. From monitoring to threat hunting, IronNet enhances IronDefense capabilities by providing customers 24/7/365 NDR services backed by Collective Defense, enabling customer SOC analysts to spend more time focusing on strategic tasks.

Table of Contents

IronNet's cybersecurity operators add to the power of IronDefense by leveraging best practices to deliver advanced NDR capabilities that meet compliance standards. Its services are scalable, measurable, and cost-effective, and they provide complete real-time visibility into the network. CyOC services include the following:

Hunt collaboration

IronNet's Hunt Team comprises highly technical security analysts with real-world operational experience in defending highly secure networks across industries and sectors. IronNet's analysts leverage its IronDefense platform to work side-by-side with customers' security operations personnel to detect and mitigate threats identified in the customer network.

Threat notifications

The CyOC team continually monitors and researches events and anomalies found in customer networks. The IronNet Customer Portal is used to notify customers of IronDefense findings of interest related to a customer's network. Notification is distributed to members determined by the customer and includes full event analysis and mitigation recommendation.

Rule deployment

The CyOC's Threat Intelligence analysts support customer operations by providing context to manual hunt operations and alert triage. The team produces tailored threat information to customer instances of IronDefense through Threat Intelligence Rule updates based on current suspicious and malicious IoCs, IronDome insights, emerging threat research, and results of research by IronNet's malware reverse engineers.

Reachback support

The CyOC team offers remote event collaboration, incident response, cybersecurity expertise, and platform support for IronDefense related security operations.

Reporting

Periodic insight reports are provided to customers on threat trends correlated to the customer's network and sector. These reports provide summarized and actionable IoCs associated with high risk network behaviors mapped to the MITRE ATT&CK Detection framework to identify the stage and progression of the threat. These reports also include a detailed list of resulting Threat Intelligence Rules deployed to customer instances of IronDefense.

Custom hunt tracking

Introductory and advanced training for end-users on analytics, alerts, entity enrichment, hunting, and network defense techniques are available. Periodic on-site side-by-side hunt operations, threat identification techniques, and review of newly implemented product features are also available.

Customer Success Team

Through IronNet's core products and services, it seeks to increase its customers' visibility into the threat landscape, reduce the impact of a potential attack and improve the overall effectiveness of cybersecurity investments. One of the ways it does this is with its dedicated Customer Success ("CS") team. While some

[Table of Contents](#)

vendors charge a premium for expert Customer Success care, IronNet includes access to its CS team as part of a customer's subscription, including a dedicated Customer Success Manager for the life of the subscription.

At the onset of a new deployment, IronNet's CS team works with customer stakeholders to map out what success looks like, determine the key deliverables required to achieve those goals and create a success plan for the life of the partnership.

Governance and Maturity Services

These services measure adherence to specific regulatory or contractual requirements and provide measurable data as to the maturity of the organization's cybersecurity capabilities.

Cybersecurity Readiness Services

Given that threat actors continuously change their tactics, techniques, and procedures ("TTP"), these services are designed to ensure organizations are prepared for the latest and most immediate threats.

Incident Response Services

IronNet provides incident response and digital forensic investigative services powered by an accomplished team with deep expertise. IronNet specializes in providing incident response and digital forensic investigative services to companies of all sizes, ranging from large U.S. Fortune 50 companies to smaller organizations.

Training

Leveraging decades of cybersecurity experience, IronNet's results-focused training programs enable customers to unlock a higher level of cyber resilience. IronNet adopts a hands-on approach to build technical proficiency and operational confidence using industry best practices. Cyber skillset training techniques include hunt methodology, offensive methodology, data analytics for security intelligence, SOC leadership, cyber threat intelligence operations, executive education, and custom cyber threat seminars.

IronNet's Customers

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust IronNet to protect their networks. The following graphic depicts representative customers of IronNet.



Customer case studies

Critical infrastructure customer case study: Southern Company

Within IronNet's first months in business, it had five major utility companies sharing cyber events in the IronDome across 25 states, helping secure infrastructure that delivers power to nearly 35 million customers.

Table of Contents

Situation: Serving nine million customers across six states, Southern Company faced risks as a target for cyber attackers to steal information or disrupt operations.

Solution: As an early adopter of Collective Defense, one of the reasons Southern Company works with IronNet is to get high quality, automated situational awareness and to move away from relying on manual methods. Southern Company invested in its partnership with IronNet to increase its ability to detect Advanced Persistent Threats, reduce dwell time and more quickly recover in the event of an attack.

IronNet's relationship with Southern Company extends beyond just a vendor/client relationship, as senior leadership from both companies appear together at numerous events and government briefings to discuss their positions on topics like nuclear energy and the security of the U.S. power grid.

Southern Company's Chief Information Security Officer notes that "Broad situational awareness within sectors and across sectors is something we believe in, and why we are doing work with IronNet and many other partners in energy and other critical sectors, both nationally and internationally."

Critical infrastructure case study: American Electric Power (AEP)

Situation: With the nation's largest transmission system consisting of more than 40,000 miles of transmission lines and more extra-high-voltage transmission lines than all other companies combined in North America, AEP needed to ensure the security of its own operations—while recognizing its role in contributing to the security of the electrical grid overall. collaborative cyber defense to combat adversaries.

Solution: Collective Defense provides the high-fidelity threat sharing to make AEP's cyber intelligence truly actionable, to ensure the cyber security of its 5.5 million customers.

AEP's Chief Security Officer says that "AEP values the relationship and initiatives being led by Gen. Alexander and IronNet."

Financial services customer case study: NBH Bank

Situation: National Bank Holdings ("NBH") needed a way to detect unknown threats. Monitoring only known threats, or "signatures" such as compromised domain names, IP addresses, or file hashes, missed a huge swath of threats that evade traditional signature-based threat detection. NBH needed a tool that could alert the security team of advanced threats across the cyber kill chain, in real time, in turn empowering the team to take action before the threat could affect operations.

Solution: After evaluating other platforms, NBH chose IronDefense for its ability to successfully detect malicious behaviors for DNS Tunneling, Domain Generation Algorithm (DGA), and Periodic Beaconing HTTP. As part of an IronDome, NBH has strengthened its ability to take proactive action against emerging threats detected by machine learning and further qualified by anonymized knowledge-sharing in the Collective Defense ecosystem.

NBH selected IronNet because of its precise analytics; proactive hunt team support; partnership with IronNet's Customer Success team; and the ability to crowdsource expertise across their peers through Collective Defense.

NBH's VP of Enterprise Technology has stated that it views IronNet's Collective Defense as the "next big thing in cyber."

Table of Contents*Sovereign wealth fund customer case study*

Situation: An Asia-Pacific-based sovereign wealth fund with a \$300 billion portfolio needed better visibility of network threats across its portfolio companies. Prior to implementing Collective Defense, neither the sovereign wealth fund nor its portfolio companies had a viable method for correlating IoCs across multiple organizations. They also lacked the ability to detect malicious threat activity based on network behaviors.

Solution: The company chose a Collective Defense IronDome to reduce time to detection via threat sharing across its portfolio companies.

In one instance, IronNet analytics detected a sinister BotNet intrusion attempt into the firm's perimeter. The detection allowed the firm to act fast and catch the BotNet on their firewall before it got inside their network – all within 24 hours of detection.

The fund's Chief Technology Officer said that "None of our other threat hunting tools sparked an alarm. This may suggest that we can turn off some of our other threat hunting tools and save some money by using IronNet. This is IronNet value at work"

In addition to becoming an IronNet customer, the sovereign wealth fund also later became an investor in IronNet.

Oil & gas customer case study

Situation: A Fortune 500 midstream natural gas and crude oil pipeline company sought to increase its detection capabilities and accelerate threat response. Other methods of information sharing proved challenging for driving real business value.

Solution: IronDome provides visibility across the sector and an instantaneous way to share anonymized threat information, allowing the company to identify unknown threats faster and react more quickly. Based on network behavior, IronNet's detection analytics help the company to maximize the value of its other cybersecurity investments by identifying potential misconfigurations or gaps to tighten overall security.

According to the company's leader of Security Operations, "IronNet is truly a partner and not just another vendor."

IronNet's Sales and Marketing***Sales***

IronNet uses a "to and through" sales strategy. By maintaining a direct sales force consisting of senior-level account executives with deep security and high-tech experience, IronNet has been able to leverage extensive professional networks and build inroads to strategic accounts. Because of this and the caliber of its senior leadership team, IronNet believes it has a differentiated ability to convene CEOs, Chief Information Security Officers (CISOs) and other leaders within an entire industry, such as energy company CEOs. This is what enables its cornerstone/community selling approach.

IronNet has three sales teams in the United States: Public Sector, covering federal, state and local segments; Critical Infrastructure, covering energy, oil & gas, and related segments; and Enterprise, covering financial services, insurance, tech, and a variety of other sectors. IronNet has direct sales staff in six countries, as well as a growing portfolio of channel, managed services and technology partners across the United States, Europe, Middle East and Africa (EMEA) and Asia-Pacific regions to scale its ability to discover, qualify, and close business.

Table of Contents

In addition, IronNet has inside sales development teams to expand its selling capabilities. These teams focus on early qualification and development of opportunities that they either close directly or transition to the field sales teams (for named accounts). These inside teams' primary objective is filling Collective Defense communities with smaller companies.

Marketing

IronNet's marketing organization employs high-tech multichannel digital and content marketing for lead generation, aggressive public relations, social media and thought leadership programs to drive awareness, and specialization in strategies such as employee advocacy and search engine optimization. IronNet was recently the top organic search engine result for "Network Detection and Response" in a competitive market.

IronNet's public relations and media program has resulted in regular coverage in business press, cybersecurity trade media and industry trade media.

IronNet's event program is focused on exposure to audiences that are aligned to its sales strategy. IronNet incorporates a combination of both large industry events like Black Hat with regional and sector-focused events that allow it to capture leads on new customers to build out Collective Defense communities. Immediately at the onset of the COVID-19 pandemic, IronNet pivoted its in-person event plan and launched a program of more than 40 webinars over the past 12 months with industry thought leaders. IronNet also regularly hosts customers on its webinars as a strategic way to create customer case studies from transcripts.

IronNet focuses on providing compelling content for both demand generation and awareness-building. Its monthly Threat Intelligence Briefs summarize the IOCs and detections its SOC has discovered in order to inform the efforts of other operations analysts in the cybersecurity space. IronNet's threat researchers produce in-depth analysis on topics such as ransomware detection and unique technical observations about the SUNBURST attack and other topics, which have been featured in media outlets. This helps build credibility with the security analyst audience, a key influencer in the buying process.

IronNet's Partnership Ecosystem

The IronNet partner ecosystem consists of leading organizations that have been carefully selected to help it deliver the power of Collective Defense across a variety of dimensions.

Technology partners

When used together, IronNet's partner integrations leverage its collective threat intelligence to react in real time, as well as proactively combat threats across the entire network, and create workflows that mitigate compromised devices. IronNet's integrations are designed to increase the efficiency of security teams with smarter, more effective workflows built through collective threat intelligence. To streamline the alert triage and incident response processes, IronDefense can integrate with a number of security products, including:

- SIEM tools to retrieve logs, share detections, and retrieve analyst feedback;
- SOAR tools to share detections, retrieve analyst feedback, and augment existing playbooks;
- EDR platforms to ingest endpoint event and entity context and initiate response to malicious activity; and
- NGFW products to dynamically block malicious activity and ingest logs for analysis.

Table of Contents

Current and planned future integrations and APIs include:

Cloud

- AWS
- Azure
- GCP

SIEM

- Splunk
- IBM QRadar
- Microsoft Azure Sentinel
- LogRhythm

SOAR

- Cortex XSOAR (formerly Demisto)
- Splunk Phantom
- Swimlane

ITSM

- ServiceNow

EDR

- CrowdStrike
- Carbon Black
- Forescout
- Tanium

NGFW

- Palo Alto Networks
- Checkpoint Software Technologies
- Zscaler

[Table of Contents](#)

partners, as well as studies of market needs, to guide product development, ensuring prioritization of new integrations, product features and functionality.

IronNet has a regular weekly cadence to report internally on its own infrastructure and security operations, as well as the health of all of its customer instances. On an annual basis, IronNet uses a third-party penetration testing team to test its environment. Additionally, IronNet uses its internal Red Team to perform quarterly testing and its Security Operations Center (“SOC”) vulnerability scans in its environment at least monthly. IronNet also monitors and reports on hunt findings and threat intelligence updates.

IronNet’s Competition

The market for IronNet’s products and services is intensely competitive and characterized by rapid changes in technology, customer requirements, and by frequent new product and service offerings and improvements. IronNet competes with a range of established and emerging security solution vendors. Conditions in its market could change rapidly and significantly as a result of technological advancements, partnerships, or acquisitions by competitors or continuing market consolidation and IronNet expects the competitive environment to remain intense.

IronNet’s competitors include the following by general category:

- First-generation NDR vendors such as DarkTrace or Vectra Networks, who offer point products based on Bayesian analysis, outlier analysis, and heuristic detection-based detection;
- Network security vendors, such as Cisco and Palo Alto Networks, Inc., who are supplementing their core network security additional behavioral-based detection with behavioral-based detection, threat intelligence and security operations solutions; and
- Legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products.

IronNet competes on the basis of a number of factors, including but not limited to its ability to:

- Detect advanced network threats and to prevent security breaches;
- Anonymously correlate and share threats in real-time across a community of peer enterprises;
- Share human-intelligence across a Collective Defense community on how peer enterprises have rated and triaged similar detections; and
- Integrate with other participants in the security ecosystem.

IronNet also competes on its:

- Time to value, price, and total cost of ownership;
- Brand awareness, reputation, and trust in IronNet’s services;
- Strength of sales, marketing, and channel partner relationships; and
- Customer success, cyber hunt, and cyber advisory services.

Although some of IronNet’s competitors enjoy greater resources, higher brand recognition, broader range of IT and security products, larger existing customer bases, or more mature intellectual property portfolios, IronNet believes that it competes favorably with respect to these factors.

[Table of Contents](#)**IRONNET'S MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS**

Unless context otherwise requires, all references in this section to "IronNet," "we," "us," "our," or "its" refer to IronNet and its consolidated subsidiaries prior to the Business Combination.

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with the consolidated financial statements and related notes thereto included elsewhere in this proxy statement/prospectus. The consolidated financial statements included elsewhere in this proxy statement/prospectus are presented in U.S. dollars (USD) rounded to the nearest thousand, with the amounts in this Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A") rounded to the nearest tenth of a million. Therefore, differences in the tables between totals and sums of the amounts listed may occur due to such rounding.

The following discussion contains forward-looking statements that involve risks and uncertainties. Our actual results could differ materially from those discussed in the forward-looking statements. Factors that could cause or contribute to these differences include those discussed below and elsewhere in this proxy statement/prospectus, particularly in the sections titled "Special Note Regarding Forward-Looking Statements" and "Risk Factors." Our fiscal year end is January 31, and our fiscal quarters end on April 30, July 31, October 31, and January 31. Our fiscal years ended January 31, 2021 and January 31, 2020 are referred to herein as fiscal 2021 and fiscal 2020, respectively. Our fiscal quarters ended April 30, 2021 and April 30, 2020 are referred to herein as fiscal quarter 2022 and fiscal quarter 2021, respectively.

Overview

Gen. Keith B. Alexander (Ret.) founded IronNet in 2014 to solve the major cybersecurity problem he witnessed and defined during his tenure as former head of the NSA and founding Commander of U.S. Cyber Command: You can't defend against threats you can't see. Our innovative approach provides the ability for groups of organizations—within an industry sector, supply chain, state or country, for example—to see, detect and defend against sophisticated cyber attacks earlier and faster than ever before.

IronNet has defined a new market category called Collective Defense. IronNet has developed the Collective Defense platform, a solution that can identify anomalous (potentially suspicious or malicious) behaviors on computer networks and share this intelligence anonymously and in real time among Collective Defense community members. Collective Defense communities comprise groups of organizations that have common risks, such as a supply chain, a business ecosystem, or across an industry sector, a state, or a country. This cybersecurity model delivers timely, actionable, and contextual alerts and threat intelligence on attacks targeting enterprise networks, and functions as an early-warning detection system for all community members.

This new platform addresses a large and unwavering compound problem: limited threat visibility for increasingly borderless enterprises across sectors and at the national level, paired with ineffective threat knowledge sharing across companies and sectors and a "go it alone" approach to cybersecurity. These operational gaps, combined with market dynamics like the increased velocity of sophisticated cyber attacks and the deepening scarcity of qualified human capital, have set our mission to transform how cybersecurity is waged.

Our Business

IronNet has focused on the development and delivery of a suite of advanced cybersecurity capabilities for detection, alerting, situational awareness and hunt/remediation combined into a comprehensive Collective Defense platform. IronNet compliments these capabilities, delivered to both commercial and public sector enterprises, with professional services.

Table of Contents

IronNet expects its capital and operating expenditures to increase significantly in connection with its ongoing activities, as IronNet:

- continues to invest in research and development related to new technologies;
- increases its investment in marketing and advertising, as well as the sales and distribution infrastructure for its products and services;
- maintains and improves operational, financial, and management information systems;
- hires additional personnel;
- obtains, maintains, expands, and protects its intellectual property portfolio; and
- enhances internal functions to support its operations as a publicly-traded company.

Impact of COVID-19 On Our Business

In December 2019, the first cases of COVID-19 were reported in China. In March 2020, the World Health Organization declared COVID-19 a global pandemic. We operate in geographic locations that have been impacted by COVID-19. The pandemic has impacted, and could further impact, our operations and the operations of our customers as a result of quarantines, various local, state and federal government public health orders, facility and business closures, and travel and logistics restrictions. We anticipate governments and businesses will likely take additional actions or extend existing actions to respond to the risks of the COVID-19 pandemic. We are continuing to actively monitor the impacts and potential impacts of the COVID-19 pandemic on our customers, supply chain, and other integral parts of our operations.

We instituted a global work-from-home policy in March 2020 and to date have not experienced significant disruptions as a result. We expect that most of our employees will work from home indefinitely. As part of our shift to remote operations, we terminated several office leases that did not have a material financial impact on us.

In response to the increased economic uncertainties that the impact of the COVID-19 pandemic may have on our business, results of operations and liquidity and capital resources, we took measures to ensure that we would be able to maintain the continuity of our business operations. For example, in April 2020 we obtained a loan in the amount of \$5.6 million from the U.S. Small Business Administration (SBA) under the Paycheck Protection Program (PPP). No payments are due under the loan until August 2021. Although we believe we remain eligible to request forgiveness of the loan amount under the rules of the SBA, we have no current intention to do so. In addition to receiving a PPP loan under the CARES Act, we also elected to defer our portion of payroll taxes due for the period from March 2020 through December 31, 2020. Of the deferred amounts, one-half will become due on each of December 31, 2021 and 2022.

Key Factors Affecting Performance***New customer acquisition***

Our future growth depends in large part on our ability to acquire new customers. If our efforts to attract new customers are not successful, our revenue may decline in the future. Our IronDefense and IronDome platforms are designed to be used in conjunction with point solutions to capture and share critical data and findings to enable our behavioral analytics to identify threats and for defenders to respond more accurately and quickly. IronNet believes that it has significant room to capture additional market share and intends to continue to invest in sales and marketing to engage its prospective customers, increase brand awareness, and drive adoption of its solution.

Customer retention

Our ability to increase revenue depends in large part on our ability to retain existing customers.

[Table of Contents](#)**Investing in business growth**

Since inception, we have invested significantly in the growth of our business. We intend to continue to invest in our research and development team to lead product improvements, our sales team to broaden our brand awareness and our general and administrative expenses to increase for the foreseeable future given the additional expenses for finance, compliance and investor relations as we grow as a public company. In addition to our internal growth, we may also consider acquisitions of businesses, technologies, and assets that complement and bolster additional capabilities to our product offerings.

Key Business Metrics

We monitor the following key metrics to measure our performance, identify trends, formulate business plans and make strategic decisions.

Recurring Software Customers

We believe that our ability to increase the number of subscription and other recurring contract type customers on our platform is an indicator of our market penetration, the growth of our business, and our potential future business opportunities. We have a history of growing the number of customers who have contracted for our platforms on a recurring basis, which does not include our professional services customers. Our recurring software customers include customers who have a recurring contract for either or both of our IronDefense and IronDome platforms. These platforms are generally sold together, but they also can be purchased on a standalone basis. We have consistently increased the number of such customers period-over-period, and we expect this trend to continue as we increase subscription offerings to small and medium-sized businesses, in addition to increased subscription offerings for our larger enterprise customers. The following table sets forth the number of recurring software customers as of the dates presented:

	Three Months Ended April 30,	
	2021	2020
Recurring Software Customers	44	20
Year-over-year growth	120%	43%
	Year Ended January 31,	
	2021	2020
Recurring Software Customers	27	20
Year-over-year growth	35%	43%

Annual Recurring Revenue ("ARR")

ARR is calculated at a particular measurement date as the annualized value of our then existing customer subscription contracts and the portions of other software and product contracts that are to be recognized over the course of the contracts and that are designed to renew, assuming any contract that expires during the 12 months following the measurement date is renewed on its existing terms. We believe this is a reasonable assumption as less than 1% of an approximate total of \$160 million in cumulative ARR that would have been reported over the last 12 quarters through the end of fiscal year 2021 did not renew the contract. The following table sets forth our ARR as of the dates presented:

	Three Months Ended April 30,	
	2021	2020
	(in millions)	
Annual recurring revenues	\$25.6	\$16.6
Year-over-year growth	54%	18%
	Year Ended January 31,	
	2021	2020
	(in millions)	
Annual recurring revenues	\$25.8	\$15.0
Year-over-year growth	72%	37%

[Table of Contents](#)

The following table presents a reconciliation of revenue, the most directly comparable financial measure calculated in accordance with GAAP, to calculated billings:

	Three Months Ended April 30,		2021 vs 2020	
	2021	2020		
	(in millions)			
Revenue	\$ 6.4	\$ 6.9	(0.5)	(7)%
Add: Total Deferred revenue, end of period	36.2	23.6	12.6	53%
Less: Total Deferred revenue, beginning of period	34.0	20.3	13.7	68%
Calculated billings	8.6	10.2	(1.6)	(16)%

	Year Ended January 31,		2021 vs 2020	
	2021	2020		
	(in millions)			
Revenue	\$29.2	\$23.2	6.1	26%
Add: Total Deferred revenue, end of period	34.0	20.3	13.7	67%
Less: Total Deferred revenue, beginning of period	20.3	20.3	0.0	0%
Calculated billings	42.9	23.2	19.7	85%

Components of Our Results of Operations

Revenue

Our revenues are derived from sales of software subscriptions, subscription-like software products and software support contracts as well as from professional services. Products, subscriptions and support revenues accounted for 96% of our revenue in fiscal quarter 2022, for 78% of our revenue in fiscal quarter 2021 and for 85% of our revenue for each of fiscal 2021 and fiscal 2020. Professional services revenues accounted for 4% of our revenue in fiscal quarter 2022, for 22% of our revenue in fiscal quarter 2021 and for 15% of our revenue for each of fiscal 2021 and fiscal 2020.

Our typical customer contracts and subscriptions range from one to five years. We typically invoice customers in advance. We combine intelligence dependent hardware and software licenses as well as subscription-type deliverables with the related threat intelligence and support and maintenance as a single performance obligation, as it delivers the essential functionality of our cybersecurity solution. Most companies also participate in the IronDome collective defense software solution that provides them access to IronNet's collective defense infrastructure linking participating stakeholders. As a result, we recognize revenue for this single performance obligation ratably over the expected term with the customer. Amounts that have been invoiced are recorded in deferred revenue or they are recorded in revenue if the revenue recognition criteria have been met. Significant judgement is required for the assessment of material rights relating to renewal options associated with our contracts.

Professional services revenues are generally sold separately from our products and include services such as development of national cyber security strategies, cyber operations monitoring, security, training, red team, incident response and tailored maturity assessments. Revenue derived from these services is recognized as the services are delivered.

Cost of Revenue

Cost of product, subscription and support revenue includes expenses related to our hosted security software, employee-related costs of our customer facing support, such as salaries, bonuses and benefits, an allocated portion of administrative costs and the amortization of deferred costs.

Cost of services revenue consists primarily of employee-related costs, such as salaries, bonuses and benefits, cost of contractors and an allocated portion of administrative costs.

[Table of Contents](#)***Gross Profit***

Gross profit, calculated as total revenue less total costs of revenue is affected by various factors, including the timing of our acquisition of new customers, renewals from existing customers, the data center and bandwidth costs associated with operating our cloud platform, the extent to which we expand our customer support organization, and the extent to which we can increase the efficiency of our technology and infrastructure through technological improvements. Also, we view our professional services in the context of our larger business and as a significant lead generator for future product sales. Because of these factors, our services revenue and gross profit may fluctuate over time.

Operating Expenses***Research and development***

Our research and development efforts are aimed at continuing to develop and refine our products, including adding new features and modules, increasing their functionality, and enhancing the usability of our platform. Research and development costs primarily include personnel-related costs and acquired software costs. Research and development costs are expensed as incurred.

Sales and marketing

Sales and marketing expenses consist primarily of employee compensation and related expenses, including salaries, bonuses and benefits for our sales and marketing employees, sales commissions that are recognized as expenses over the period of benefit, marketing programs, travel and entertainment expenses, and allocated overhead costs. We capitalize our sales commissions and recognize them as expenses over the estimated period of benefit.

We intend to continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market and expand our global customer base. In particular, we will continue to invest in growing and training our sales force, broadening our brand awareness and expanding and deepening our channel partner relationships. We expect our sales and marketing expenses to decrease as a percentage of our revenue over the long term, although our sales and marketing expenses may fluctuate as a percentage of our revenue from period to period due to the timing and extent of these expenses.

General and administrative

General and administrative costs include salaries, stock-based compensation expenses, and benefits for personnel involved in our executive, finance, legal, people and culture, and administrative functions, as well as third-party professional services and fees, and overhead expenses.

We expect that general and administrative expenses will increase in absolute dollars as we hire additional personnel and enhance our systems, processes, and controls to support the growth in our business as well as our increased compliance and reporting requirements as a public company.

Other income (expense), net

Other income (expense), net consists primarily of interest income, interest expense, and foreign currency exchange gains and losses.

Provision for income taxes

Provision for income taxes consists of federal and state income taxes in the United States and income taxes and withholding taxes in certain foreign jurisdictions in which we conduct business. We maintain a full valuation allowance on our U.S. federal and state deferred tax assets.

[Table of Contents](#)**Results of Operations****Comparison of Fiscal Quarter 2022 and Fiscal Quarter 2021**

The following tables set forth our consolidated statements of operations in dollar amounts and as a percentage of total revenue for each period presented (dollars in millions):

	Three Months Ended April 30,				2021 vs	
	2021		2020		2020	
	(in millions)					
Software, subscription and support revenue	\$ 6.1	95%	\$ 5.4	78%	\$ 0.7	13%
Professional services revenue	0.2	3%	1.5	22%	(1.2)	(87%)
Total revenue	6.4	100%	6.9	100%	(0.5)	(7%)
Cost of software, subscription and support revenue	1.8	28%	1.5	22%	0.3	20%
Cost of service revenue	0.2	3%	0.3	4%	(0.1)	(33%)
Total cost of revenue	1.9	30%	1.8	26%	0.1	6%
Gross profit	4.4	69%	5.0	72%	(0.6)	(12%)
Operating expenses:						
Research and development	6.9	104%	7.4	108%	(0.5)	(7%)
Sales and marketing	7.1	112%	8.2	120%	(1.1)	(13%)
General and administrative	5.7	90%	5.8	84%	(0.1)	(1%)
Total operating expenses	19.8	305%	21.4	312%	(1.6)	(7%)
Operating loss	(15.3)	(235%)	(16.4)	(239%)	1.1	(7%)
Other (expense) income, net	(0.1)	(2%)	0.0	0%	(0.1)	nm
Loss before provision for income taxes	(15.4)	(237%)	(16.4)	(239%)	1.0	(6%)
Provision for income taxes	(0.1)	(1%)	(0.0)	0%	(0.1)	211%
Net loss	\$(15.5)	(238%)	\$(16.4)	(239%)	\$ 0.9	(5%)

nm - not meaningful

Revenue

Total revenue decreased by \$0.5 million or (7)% in fiscal quarter 2022 compared to fiscal quarter 2021 due to lower Professional services revenue compared to atypically higher services in the same period last year.

Software revenue increased by a net of 13% even while the company completed its transition from contracts that had material non-recurring elements to contract forms that were fully designed to renew. As our initial contract terms with legacy customers have expired, renewals of those customers have preserved and extended the recurring elements of those engagements.

Of the overall growth in software revenue, the subscription revenue portion increased by \$2.7 million or 79%, in fiscal quarter 2022, from \$3.4 million to \$6.1 million and accounted for 99% of our total software revenue in fiscal quarter 2022, up from 63% in fiscal quarter 2021. A disproportionate amount of that growth compared to the same quarter of last year has come from new customers in the Asia-Pacific region. New customers, worldwide, accounted for \$2.5 million of the subscription revenue increase, and existing customers accounted for a net increase of \$0.2 million of the year over year growth. The \$2.7 million increase in subscription revenue portion of our software revenue was offset by a \$2.0 million decrease in non-recurring revenue as we completed our transition to recurring revenue type contracts. Software, subscription and support revenue overall accounted for 95% of our total revenue in fiscal quarter 2022 and for 78% of our total revenue in fiscal quarter 2021.

Professional services revenue decreased \$1.2 million or 87% in fiscal quarter 2022 compared to fiscal quarter 2021, primarily due to the completion of a national cybersecurity strategy engagement in EMEA in fiscal 2021 and delays in professional services contract starts in fiscal quarter 2022 due to lockdowns from COVID-19. Professional services accounted for 3% of our total revenue in fiscal quarter 2022 and for 22% of our total revenue in fiscal quarter 2021.

[Table of Contents](#)**Cost of revenue**

Total cost of revenue increased by \$0.1 million or 6%, in fiscal quarter 2022, compared to fiscal quarter 2021. Cost of software, subscription and support revenue increased by \$0.3 million or 20%, in fiscal quarter 2022, compared to fiscal quarter 2021. The increase was due primarily to an increase in overall product, subscription and support sales in fiscal quarter 2022 compared to fiscal quarter 2021.

Cost of service revenue decreased by \$0.1 million or (33)% in fiscal quarter 2022, compared to fiscal quarter 2021. The decrease in cost of service revenue was primarily due to a decrease in overall professional services activity in fiscal quarter 2022 compared to fiscal quarter 2021.

Gross Profit and Gross Margin

Mix changes in cost of revenue resulted in a small decrease in software gross margin to 70.5% in fiscal quarter 2022 compared to 72.2% in fiscal quarter 2021. We expect that gross margins for the rest of fiscal 2022 will improve and be above the fiscal 2021 level. However, margins may remain volatile compared to fiscal 2021 due to the continuing presence of large contracts in our revenue mix.

The following tables show gross profit and gross margin, respectively, for software products and support revenue and professional services revenue for fiscal quarter 2022 as compared to fiscal quarter 2021.

	Three Months Ended April 30,		2021 vs 2020	
	2021	2020		
	(in millions)			
Software products margin	\$ 4.4	\$ 3.9	\$ 0.5	13%
Professional services margin	—	1.2	(1.2)	(100%)
Total Gross profit margin	4.4	5.1	(0.7)	(14%)
	2021	2020	Change	
Software products margin	71.4%	71.6%	(0.2%)	
Professional services margin	23.3%	78.1%	(55.4%)	
Total Gross profit margin	69.6%	73.1%	(3.5%)	

Operating expenses**Research and development**

Research and development expenses decreased by \$0.5 million or (7)%, in fiscal quarter 2022, compared to fiscal quarter 2021 primarily due to the increased capitalization of research and development payroll. At 104% of total revenues in fiscal quarter 2022 compared to 108% in fiscal quarter 2021, we expect that our overall R&D expenditure rate as a percentage of sales will decline in the future.

Sales and marketing

Sales and marketing cost decreased by \$1.1 million or (13)% in fiscal quarter 2022, compared to fiscal quarter 2021, primarily due to a large number of newly hired but not yet trained sales and marketing personnel in fiscal quarter 2021 which, decreased 20% over the course of the fiscal year as the company settled on its highest performing personnel. This led to a 11% decrease in sales and marketing payroll costs in fiscal quarter 2022 compared to the comparable prior quarter. At 112% of total revenues in fiscal quarter 2022 compared to 120% in fiscal quarter 2021, we expect that our overall sales and marketing expenditure rates as a percentage of revenues will continue to decline in the future.

General and administrative

General and administrative costs decreased by \$0.1 million or (1)% in fiscal quarter 2022, compared to fiscal quarter 2021, including the one-time charges relating to the proposed combination of \$0.6 million. This fluctuation

[Table of Contents](#)**SIGNATURES**

Pursuant to the requirements of the Securities Act, the registrant has duly caused this registration statement to be signed on its behalf by the undersigned, thereunto duly authorized, in New York, NY, on the 6th day of August, 2021.

LGL SYSTEMS ACQUISITION CORP.

By: /s/ Robert LaPenta Jr.
 Robert LaPenta Jr.
 Co-Chief Executive Officer and Chief Financial Officer

Pursuant to the requirements of the Securities Act of 1933, this registration statement has been signed by the following persons in the capacities and on the dates indicated.

<u>Name</u>	<u>Title</u>	<u>Date</u>
<u>/s/ Marc J. Gabelli</u> Marc J. Gabelli	Chairman and Co-Chief Executive Officer (Co-Principal Executive Officer)	August 6, 2021
<u>/s/ Robert LaPenta Jr.</u> Robert LaPenta Jr.	Co-Chief Executive Officer and Chief Financial Officer (Co-Principal Executive Officer and Principal Accounting and Financial Officer)	August 6, 2021
<u>*</u> Mary E. Gallagher	Director	August 6, 2021
<u>*</u> Michael Ferrantino	Director	August 6, 2021
<u>*</u> Michael Martin	Director	August 6, 2021
<u>* By /s/ Robert LaPenta Jr.</u> Robert LaPenta Jr. Attorney-in-fact		

INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM'S CONSENT

We consent to the inclusion in this Registration Statement of LGL Systems Acquisition Corp. on Amendment 3 to Form S-4 (File No. 333-256129) of our report dated March 3, 2021, except for the merger agreement disclosed in Note 12 and for effects of the restatement discussed in Notes 2, 8, 9, 10, and 11, as to which the date is May 10, 2021, with respect to our audits of the financial statements of LGL Systems Acquisition Corp. as of December 31, 2020 and 2019, for the year ended December 31, 2020 and for the period from April 30, 2019 (inception) through December 31, 2019, which report appears in the Prospectus, which is part of this Registration Statement. We also consent to the reference to our Firm under the heading "Experts" in such Prospectus.
/s/ Marcum LLP

Marcum LLP
Houston, TX
August 6, 2021

Exhibit 23.3

CONSENT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

We hereby consent to the use in this Amendment No. 3 to the Registration Statement on Form S-4 of LGL Systems Acquisitions Corp. of our report dated May 14, 2021 relating to the financial statements of IronNet Cybersecurity, Inc., which appears in this Registration Statement. We also consent to the reference to us under the heading “Experts” in such Registration Statement.

/s/ PricewaterhouseCoopers LLP

Baltimore, Maryland
August 6, 2021